



SAPIENZA
UNIVERSITÀ DI ROMA

“SAPIENZA” UNIVERSITÀ DI ROMA
INGEGNERIA DELL'INFORMAZIONE,
INFORMATICA E STATISTICA
DIPARTIMENTO DI INFORMATICA

Algebra

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

Author
Simone Bianco

25 settembre 2023

Indice

Informazioni e Contatti	1
1 Strutture algebriche principali	2
1.1 Operazioni binarie e loro proprietà	2
1.2 Gruppi, Anelli e Campi	5
1.3 Sottogruppi ed Ideali	8
2 Numeri Complessi	11
2.1 Il campo dei numeri complessi	11
2.2 Forma polare dei numeri complessi	14
2.3 Teorema fondamentale dell'algebra	18
3 Relazioni e Induzione	20
3.1 Classi di equivalenza	22
3.2 Relazione di Divisore	25
3.3 Relazione di Congruenza	26
3.4 Teorema della divisione con resto euclidea	27
3.5 Relazione di Coniugio	28
3.6 Induzione matematica	29
4 Elementi di Teoria degli Anelli	33
4.1 Classi laterali sinistre	33
4.1.1 Teorema di Lagrange	35
4.2 L'anello commutativo \mathbb{Z}_n	36
4.3 Invertibili e Divisori dello zero	38
4.4 Elementi irriducibili e primi	42
4.5 Massimo comun divisore	45
4.5.1 Algoritmo di Euclide	48
4.5.2 Criteri di divisibilità	52
4.6 Minimo comune multiplo	53
4.7 Teorema fondamentale dell'aritmetica	55
4.8 Teorema cinese dei resti	58
4.9 Piccolo teorema di Fermat	65
4.10 Funzione totiente di Eulero	69
4.11 Ordine di un elemento di un gruppo	71

5	Gruppo Simmetrico	80
5.1	Ordine di una permutazione	83
5.2	Segno delle permutazioni	86
6	Morfismi	94
6.1	Isomorfismi, Endomorfismi ed Automorfismi	96
6.2	Nucleo ed Immagine di un morfismo	100
6.3	Primo teorema d'isomorfismo	101
6.4	Sottogruppi normali	103
6.5	Gruppi diedrali	110
6.6	Gruppo di Klein e Teorema di Cauchy	114
7	Polinomi	120
7.1	Divisione con resto di polinomi	123
7.2	Proprietà dell'anello polinomiale	126
7.3	Polinomi in \mathbb{Z}_p	134
8	Spazi vettoriali	137
8.1	Span, Generatori e Indipendenza lineare	139
8.2	Base e Dimensione	143
8.2.1	Formula di Grassman	147
8.3	Trasformazioni lineari	149
8.3.1	Teorema del Rango	153
8.4	Spazi affini, Sottospazi affini e Giacitura	154
8.5	Prodotto scalare e Spazio ortogonale	155
9	Matrici	158
9.1	Rango di una matrice	162
9.1.1	Riduzione a scala di una matrice	164
9.2	Teorema di Rouché-Capelli	168
9.2.1	Equazioni parametriche	170
9.3	Determinante di una matrice	172
9.3.1	Formula di Leibniz e Regola di Sarrus	174
9.3.2	Determinante tramite riduzione a scala	176
9.3.3	Sviluppo di Laplace	178
9.3.4	Regola di Cramer	180
9.4	Matrici inverse	181
9.5	Teorema degli orlati	188
9.6	Matrici simili	194
9.6.1	Diagonalizzazione di una matrice	200
9.7	Matrice di una trasformazione lineare	206
9.8	Matrici ortogonali	212
10	Algoritmi di crittografia	216
10.1	Algoritmo RSA	216
10.2	Interpolazione di Lagrange e Algoritmo SSS	218

Informazioni e Contatti

Appunti e riassunti personali raccolti in ambito del corso di *Algebra* offerto dal corso di laurea in Informatica dell'Università degli Studi di Roma "La Sapienza".

Ulteriori informazioni ed appunti possono essere trovati al seguente link:

<https://github.com/Exyss/university-notes>. Chiunque si senta libero di segnalare incorrettezze, migliorie o richieste tramite il sistema di Issues fornito da GitHub stesso o contattando in privato l'autore :

- Email: bianco.simone@outlook.it
- LinkedIn: [Simone Bianco](#)

Gli appunti sono in continuo aggiornamento, pertanto, previa segnalazione, si prega di controllare se le modifiche siano già state apportate nella versione più recente.

Prerequisiti consigliati per lo studio:

Apprendimento del materiale relativo al corso *Metodi Matematici per l'Informatica*.

Licence:

These documents are distributed under the [GNU Free Documentation License](#), a form of copyleft intended for use on a manual, textbook or other documents. Material licensed under the current version of the license can be used for any purpose, as long as the use meets certain conditions:

- All previous authors of the work must be **attributed**.
- All changes to the work must be **logged**.
- All derivative works must be **licensed under the same license**.
- The full text of the license, unmodified invariant sections as defined by the author if any, and any other added warranty disclaimers (such as a general disclaimer alerting readers that the document may not be accurate for example) and copyright notices from previous versions must be maintained.
- Technical measures such as DRM may not be used to control or obstruct distribution or editing of the document.

1

Strutture algebriche principali

1.1 Operazioni binarie e loro proprietà

Definizione 1: Operazione binaria

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

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

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

Osservazione 1

Per leggibilità, d'ora in poi indicheremo l'applicazione di un'operazione binaria generica $m(x, y)$ come xy .

Tuttavia, tale notazione 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** e l'**operazione moltiplicativa**, ossia:

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

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

sono entrambe operazioni binarie.

- Sull'insieme $X = \{f \mid f : S \rightarrow S : x \mapsto y\}$ (dove S è un insieme qualsiasi) la **composizione tra funzioni**, ossia:

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

è un'operazione binaria.

- Sull'insieme \mathbb{N} , l'**operazione sottrazione**, ossia:

$$- : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} : (x, y) \mapsto x - y$$

non è un'operazione binaria

Definizione 2: Proprietà associatività

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

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

Esempi:

- L'operazione additiva $+$: $\mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ gode della proprietà associativa:

$$\forall x, y, z \in \mathbb{R} \quad (x + y) + z = x + (y + z) = x + y + z$$

- L'operazione moltiplicativa \cdot : $\mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ gode della proprietà associativa:

$$\forall x, y, z \in \mathbb{R} \quad (x \cdot y) \cdot z = x \cdot (y \cdot z) = x \cdot y \cdot z$$

Definizione 3: Esistenza dell'elemento neutro

Data un'operazione binaria $m : S \times S \rightarrow S$, tale operazione gode dell'**esistenza dell'elemento neutro** se

$$\exists! e \in S \mid \forall x \in S \quad xe = ex = x$$

dove e viene detto **elemento neutro**.

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:

- Nell'operazione additiva $+: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$, l'elemento neutro è 0 poiché

$$\forall x \in \mathbb{R} \quad x + 0 = 0 + x = x$$

- Nell'operazione moltiplicativa $\cdot: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$, l'elemento neutro è 1 poiché

$$\forall x \in \mathbb{R} \quad x \cdot 1 = 1 \cdot x = x$$

Definizione 4: Esistenza dell'elemento inverso

Data un'operazione binaria $m: S \times S \rightarrow S$, tale operazione gode dell'**esistenza dell'elemento inverso** se

$$\forall x \in S \quad \exists! x^{-1} \in S \mid xx^{-1} = x^{-1}x = e$$

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:

- L'operazione additiva $+: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ gode dell'esistenza dell'elemento inverso poiché

$$\forall x \in \mathbb{R} \quad \exists! -x \in \mathbb{R} \mid x + (-x) = (-x) + x = 0$$

- L'operazione moltiplicativa $\cdot: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ gode dell'esistenza dell'elemento inverso poiché

$$\forall x \in \mathbb{R} \quad \exists! \frac{1}{x} \in \mathbb{R} \mid x \cdot \frac{1}{x} = \frac{1}{x} \cdot x = 1$$

Osservazione 2

Se un'operazione binaria gode dell'**esistenza dell'elemento inverso**, allora essa gode necessariamente anche dell'**esistenza dell'elemento neutro**

Definizione 5: Proprietà commutativa

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

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

Esempi:

- L'operazione additiva $+: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ gode della proprietà commutativa:

$$\forall x \in \mathbb{R} \quad x + y = y + x$$

- L'operazione moltiplicativa $\cdot : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ gode della proprietà commutativa:

$$\forall x \in \mathbb{R} \quad x \cdot y = y \cdot x$$

1.2 Gruppi, Anelli e Campi

Definizione 6: Strutture algebriche semplici

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

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

Esempi:

- $(\mathbb{N} - \{0\}, +)$ è un **semigrupp**
- $(\mathbb{N}, +)$ è un **monoide** commutativo
- (\mathbb{R}, \cdot) è un **gruppo abeliano**
- (\mathbb{Z}, \cdot) è un **monoide** commutativo

- Dato l'insieme X , definiamo X^X come l'insieme di tutte le funzioni da X ad X , ossia $X^X := \{f \mid f : X \rightarrow X\}$.

La struttura algebrica (X^X, \circ) è un monoide, poiché gode di:

– **Associatività:**

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

– **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 tale che $\forall x \in X$ valga $\text{id}(x) = x$.

Definizione 7: Anello

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

- $(A, +)$ è un **gruppo abeliano**
- (A, \cdot) è un **monoide**
- Gode della **proprietà distributiva**, definita come:

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

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

In particolare, definiamo un anello come **anello commutativo** se in (A, \cdot) vale anche l'**assioma di commutatività** (dunque se (A, \cdot) è un monoide commutativo)

Proposizione 1

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

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

Dimostrazione:

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

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

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

□

Proposizione 2

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

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

Dimostrazione:

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

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

□

Corollario 1

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

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

Definizione 8: Campo

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

- $(K, +, \cdot)$ è un **anello commutativo**
- $\forall x \in K - \{0\} \quad \exists! x^{-1} \in K - \{0\} \mid xx^{-1} = x^{-1}x = e$

Esempi:

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

1.3 Sottogruppi ed Ideali

Definizione 9: Sottogruppo

Dato un gruppo (G, \cdot) , definiamo (H, \cdot) come **sottogruppo** di G , indicato come $H \leq G$, se:

- $H \subseteq G$
- $e \in H$, 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:

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

Definizione 10: Ideale

Dato un anello $(A, +, \cdot)$, definiamo $(I, +, \cdot)$ come **ideale** di A , indicato come $I \triangleleft A$, se:

- $I \subseteq A$
- $(I, +) \leq (A, +)$
- $AI \subseteq I$, dove $AI := \{ax \mid x \in I, a \in A\}$
- $IA \subseteq I$, dove $IA := \{yb \mid y \in I, b \in A\}$

Attenzione: generalmente, si ha che $AI \neq IA$

Osservazione 3

Sia A un anello e sia $I \triangleleft A$. Se A è **commutativo**, allora I è **commutativo**

Definizione 11: Ideale generato da elementi

Sia A un anello commutativo e siano $a_1, \dots, a_n \in A$. Definiamo $I(a_1, \dots, a_n) \triangleleft A$ come **ideale generato da** a_1, \dots, a_n , dove

$$I(a_1, \dots, a_n) := \{a_1b_1 + \dots + a_nb_n \mid b_1, \dots, b_n \in A\}$$

Dimostrazione:

- 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:

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

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

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

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

$$\begin{aligned} x \in I(a_1, \dots, a_n) &\iff x = a_1 b_1 + \dots + a_n b_n \implies c \in A \mid cx = c(a_1 b_1 + \dots + a_n b_n) \\ &\implies cx = c(a_1 b_1 + \dots + a_n b_n) = a_1(b_1 c) + \dots + a_n(b_n c) \implies cx \in I(a_1, \dots, a_n) \end{aligned}$$

□

Definizione 12: Ideale principale

Sia A un anello commutativo. Definiamo $I(a) \triangleleft A$ come **ideale principale di A generato da a** , dove $I(a)$ ricordiamo essere definito come:

$$I(a) = \{ax \mid x \in A\}$$

Proposizione 3: Somma tra ideali

Dato un anello commutativo A e due suoi ideali $I, J \triangleleft A$, si ha che $I + J \triangleleft A$, dove:

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

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:

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

□

Proposizione 4: Intersezione tra ideali

Dato un anello commutativo A e due suoi ideali $I, J \triangleleft A$, si ha che $I \cap J \triangleleft A$, dove:

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

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:

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

□

Proposizione 5: Prodotto tra ideali

Dato un anello commutativo A e due suoi ideali $I, J \triangleleft A$, si ha che $I \cdot J \triangleleft A$, dove:

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

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:

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

□

2

Numeri Complessi

2.1 Il campo dei numeri complessi

Definizione 13: Numeri complessi

Definiamo l'insieme dei **numeri complessi** come:

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

dove il simbolo i è l'**unità immaginaria**, per cui si ha che $i^2 = -1$.

Inoltre, si ha che $\mathbb{R} \subseteq \mathbb{C}$.

Definizione 14: Parte reale e Parte immaginaria

Dato $z := a + ib \in \mathbb{C}$, definiamo:

- $Re(z)$ come **parte reale di z** , dove $Re(z) = a$
- $Im(z)$ come **parte immaginaria di z** , dove $Im(z) = b$

Inoltre, definiamo z come **numero immaginario puro** se $Re(z) = 0$ e $Im(z) \neq 0$

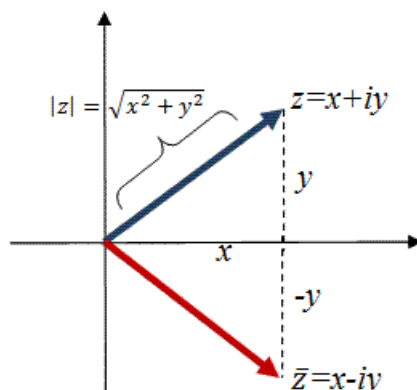
Definizione 15: Coniugato di un numero complesso

Dato $z := a + ib \in \mathbb{C}$, definiamo $\bar{z} \in \mathbb{C}$ come **coniugato di z** se

$$\bar{z} = a - ib$$

ossia se $Re(\bar{z}) = Re(z)$ e $Im(\bar{z}) = -Im(z)$

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 la **distanza euclidea**:

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

Proposizione 6

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

1. $\bar{z} + \bar{w} = \overline{z + w}$
2. $\bar{z} \cdot \bar{w} = \overline{zw}$
3. $z \cdot \bar{z} = |z|^2$

Dimostrazione:

- Dati $z := a + ib \in \mathbb{C}$ e $w := c + id \in \mathbb{C}$, si ha che
 1. $\bar{z} + \bar{w} = a - ib + c - id = (a + c) - i(b + d) = \overline{z + w}$
 2. $\bar{z} \cdot \bar{w} = (a - ib)(c - id) = (ac - bd) - i(ad + bc) = \overline{zw}$
 3. $z \cdot \bar{z} = (a + ib)(a - ib) = a^2 - (ib)^2 = a^2 + b^2 = |z|^2$

Proposizione 7

La struttura algebrica $(C, +, \cdot)$ 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**:

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

- Dimostriamo quindi che $(\mathbb{C}, +, \cdot)$ sia un anello commutativo:

– **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**

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

– **Elemento inverso della somma**

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

– **Commutatività della somma**

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

– **Associatività del prodotto**

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

– **Elemento neutro del prodotto**

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

– **Commutatività del prodotto**

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

- Dato $z := a + ib \in \mathbb{C}$, consideriamo il suo possibile inverso, ossia l'elemento $z^{-1} = \frac{1}{a+ib}$, il quale non appare nella forma $c + id \mid c, d \in \mathbb{R}$ richiesta dalla definizione di insieme dei numeri complessi.

- Riscriviamo quindi z^{-1} come:

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

- A questo punto, ponendo $c := \frac{a}{a^2 + b^2} \in \mathbb{R}$ e $d := \frac{-b}{a^2 + b^2} \in \mathbb{R}$, otteniamo che $z^{-1} = c + id \in \mathbb{C}$, rientrando quindi nella definizione corretta di insieme dei numeri complessi
- Per tanto, si ha che:

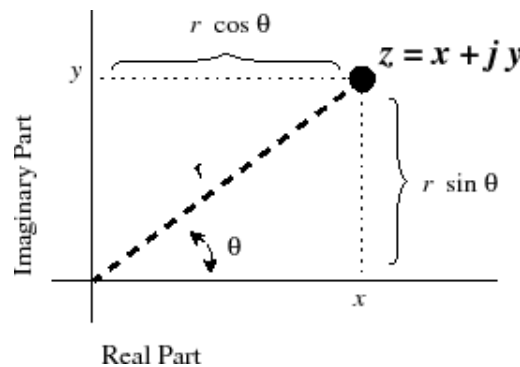
$$\forall z \in \mathbb{C} - \{0\} \quad \exists! z^{-1} := \frac{a}{a^2 + b^2} + i \cdot \frac{-b}{a^2 + b^2} \mid z \cdot z^{-1} = 1$$

implicando dunque che valga anche l'assioma di elemento inverso del prodotto e di conseguenza che \mathbb{C} sia un campo. □

2.2 Forma polare dei numeri complessi

Abbiamo già trattato di 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 identificare 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 .



Di conseguenza, dato $r = |z|$ abbiamo che:

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

Definizione 16: Argomento di un numero complesso

Dato $z := a + ib \in \mathbb{C}$, definiamo come **argomento di z** , indicato come $\arg(z)$, una qualsiasi soluzione valida al seguente sistema:

$$\begin{cases} \cos(\arg(z)) = \frac{a}{|z|} \\ \sin(\arg(z)) = \frac{b}{|z|} \end{cases}$$

Osservazione 4

Dato $z := a + ib \in \mathbb{C}$, esistono **infiniti argomenti di z** .

Dimostrazione:

- Sia $\theta \in \mathbb{R}$ un argomento di z , ossia tale che:

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

- Essendo le funzioni seno e coseno periodiche, $\forall k \in \mathbb{Z}$ si ha che:

$$\begin{cases} \cos(\theta) = \cos(\theta + 2k\pi) \\ \sin(\theta) = \sin(\theta + 2k\pi) \end{cases} \implies \begin{cases} \cos(\theta + 2k\pi) = \frac{a}{|z|} \\ \sin(\theta + 2k\pi) = \frac{b}{|z|} \end{cases}$$

□

Definizione 17: Argomento principale di un numero complesso

Dato $z := a + ib \in \mathbb{C}$, definiamo come **argomento principale di z** , indicato come $\text{Arg}(z)$, l'unico argomento di z tale che $\text{Arg}(z) \in [0, 2\pi]$

Teorema 1: Formula di Eulero

Dato un angolo $\theta \in \mathbb{R}$, si ha che

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

(*dimostrazione omessa*)

Corollario 2: Formula di De Moivre

Dato un angolo $\theta \in \mathbb{R}$ e $n \in \mathbb{Z}$, si ha che

$$(\cos(\theta) + i \cdot \sin(\theta))^n = \cos(n\theta) + i \cdot \sin(n\theta)$$

Dimostrazione:

- Tramite la formula di Eulero, si ha che:

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

□

Proposizione 8: Forma polare di un numero complesso

Dato $z \in \mathbb{C}$ e posti $r := |z|$ e $\theta := \text{Arg}(z)$, si ha che

$$z = r(\cos(\theta) + i \cdot \sin(\theta)) = re^{i\theta}$$

Inoltre, definiamo tali altre due rappresentazioni di z come **forma polare di z**

Dimostrazione:

- Rappresentando z sul piano di Gauss, si ha che:

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

- Infine, per la formula di Eulero si ha che:

$$z = r(\cos(\theta) + i \cdot \sin(\theta)) = re^{i\theta}$$

□

Osservazione 5: Operazioni in forma polare

Dati $z, w \in \mathbb{C}$ e posti $r_1 := |z|$, $\theta_1 := \text{Arg}(z)$ e $r_2 := |w|$, $\theta_2 := \text{Arg}(w)$, si ha che:

1. $z \cdot w = r_1 r_2 e^{i(\theta_1 + \theta_2)}$
2. $\frac{z}{w} = \frac{r_1}{r_2} e^{i(\theta_1 - \theta_2)}$
3. $z^n = r_1^n e^{in\theta_1}$, dove $n \in \mathbb{Q}$

Attenzione: eccetto rari casi, per calcolare prodotti o divisioni tra numeri complessi risulta essere comunque più comodo calcolare il prodotto tramite la proprietà distributiva e la divisione riscrivendo $\frac{1}{w}$ come $\frac{a}{a^2+b^2} + i \cdot \frac{-b}{a^2+b^2}$, dove $w := a + ib$

Esempi:

1. Dato $z = -i$, calcolare z^4 .
 - Calcoliamo l'argomento principale di z :

$$r := |z| = \sqrt{0^2 + (-1)^2} = 1 \implies \begin{cases} \cos(\theta) = \frac{0}{1} = 0 \\ \sin(\theta) = \frac{-1}{1} = -1 \end{cases} \implies \text{Arg}(z) = \frac{3}{2}\pi$$

- Di conseguenza, otteniamo che

$$z = re^{\operatorname{Arg}(z) \cdot i} = e^{\frac{3}{2}\pi \cdot i} \implies z^4 = e^{4 \cdot \frac{3}{2}\pi \cdot i} = e^{6\pi \cdot i} = e^{0 \cdot i} = 1$$

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

- Calcoliamo l'argomento principale di z :

$$r := |z| = \sqrt{1^2 + (-1)^2} = \sqrt{2} \implies \begin{cases} \cos(\theta) = \frac{1}{\sqrt{2}} \\ \sin(\theta) = \frac{-1}{\sqrt{2}} \end{cases} \implies \text{Arg}(z) = \frac{7}{4}\pi$$

- Di conseguenza, otteniamo che

$$z = re^{\text{Arg}(z) \cdot i} = \sqrt{2}e^{\frac{7}{4}\pi \cdot i} \implies z^{10} = (\sqrt{2})^{10}e^{10 \cdot \frac{7}{4}\pi \cdot i} = 2^5e^{\frac{35}{2}\pi i} = 2^5e^{\frac{3}{2}\pi i}$$

- Avendo già visto precedentemente che $e^{\frac{3}{2}\pi i} = -i$, otteniamo che:

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

2.3 Teorema fondamentale dell'algebra

Dati $z \in \mathbb{C}$ e $n \in \mathbb{N} \mid n \geq 2$, ci chiediamo quante siano le **soluzioni complesse all'equazione** $x^n = z$:

- Se $z = 0$, l'unica soluzione risulta essere $x = 0$
- Consideriamo quindi il caso in cui $z \neq 0$. Tramite la formula di De Moivre, possiamo riscrivere tale equazione come:

$$x^n = z \iff x = \sqrt[n]{z} \iff x = z^{\frac{1}{n}} \iff x = r^{\frac{1}{n}}e^{\frac{1}{n}\theta i}$$

ottenendo quindi una soluzione valida all'equazione.

- Tuttavia, ricordando che un numero complesso z possiede **infiniti argomenti**, riscriviamo x nella forma più generica:

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

- A questo punto, al variare di $k = 0, 1, \dots, n-1$ è possibile trovare le **uniche n soluzioni distinte 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 $k = 3$

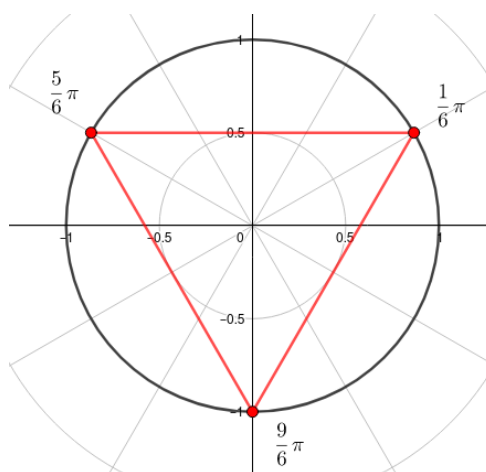
$$x_4 = e^{i(\frac{1}{2 \cdot 3}\pi + \frac{6\pi}{3})} = e^{i(\frac{1}{6}\pi + 2\pi)} = e^{\frac{1}{6}\pi i} \implies x_4 = x_1$$

– 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**.
- 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:



Osservazione 6

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 $|z|^{\frac{1}{n}}$.

Teorema 2: 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 $p(x)$:

$$\forall i \in [1, n] \quad \exists x_1, \dots, x_n \in \mathbb{C} \mid p(x_i) = 0$$

3

Relazioni e Induzione

Definizione 18: 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 $\neg R(x, y)$).

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

Definizione 19: Relazione di equivalenza

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

- **Riflessività:** $\forall x \in X \quad x \sim x$
- **Simmetria:** $\forall x, y \in X \quad x \sim y \implies y \sim x$
- **Transitività:** $\forall x, y, z \in X \quad x \sim y, y \sim z \implies x \sim z$

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

Definizione 20: Relazione d'ordine totale e parziale

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

- **Riflessività:** $\forall x \in X \quad x \prec x$
- **Anti-simmetria:** $\forall x, y \in X \quad x \prec y, y \prec x \implies x = y$
- **Transitività:** $\forall x, y, z \in X \quad x \prec y, y \prec z \implies x \prec z$
- **Totalità:** $\forall x, y \in X \quad x \prec y \vee y \prec x$

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 $a \leq b$ 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

Definizione 21: 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 :

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

Osservazione 7

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

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

Definizione 22: 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:

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

Definizione 23: 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 :

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

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

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

Osservazione 8

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:

$$[x] \cap [y] \neq \emptyset \iff \exists z \in [x] \cap [y] \iff z \in [x] \wedge z \in [y] \iff$$

$$\iff z \sim x, z \sim y \iff x \sim z, z \sim y \implies x \sim y$$

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 $[x] \cap [y] = \emptyset \implies x \not\sim y$

□

Corollario 3

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:

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

□

Proposizione 9

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:

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

□

Proposizione 10: 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

Definizione 24: 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"

Osservazione 9

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

$$\begin{aligned} n \neq 0 &\implies n = n(pq) \implies qp = 1 \implies p = q = \pm 1 \implies \\ &\implies \begin{cases} n = m & \text{se } p = q = 1 \\ n = -m & \text{se } p = q = -1 \end{cases} \end{aligned}$$

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

□

Corollario 4

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

Definizione 25: 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 $a \equiv b \pmod{n}$, se e solo se $n \mid b - a$

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

Esempi:

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

Osservazione 10

La relazione di congruenza $a \equiv b \pmod{n}$ è una **relazione di equivalenza**.

Dimostrazione:

- **Riflessiva:**

$$a = a \iff a = n \cdot 0 + a \iff a - a = n \cdot 0 \iff n \mid a - a \iff a \equiv a \pmod{n}$$

- **Simmetrica:**

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

- **Transitiva:**

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

3.4 Teorema della divisione con resto euclidea

Teorema 3: 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:

$$\exists r \in [m]_{\geq 0} \mid r = \min([m]_{\geq 0}) \implies \exists q \in \mathbb{Z} \mid r = m - nq$$

- Supponiamo per assurdo che $r \geq n$, da cui ne segue che $r - n \geq 0 \implies r - n \in \mathbb{N}$. Dunque, abbiamo che:

$$r - n = (m - nq) - n \iff r - n = m - n(q + 1) \iff r - n \in [m]_{\geq 0}$$

- Poiché $r - n \leq r$, l'ipotesi per cui r sia il minimo di $m_{\geq 0}$ viene contraddetta, 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:

$$\begin{aligned} \exists q_1, q_2, r_1, r_2 \in \mathbb{Z}, 0 \leq r_1, r_2 < n \mid nq_1 + r_1 = m = nq_2 + r_2 &\implies \\ \implies nq_1 + r_1 = nq_2 + r_2 &\implies r_2 - r_1 = n(q_1 - q_2) \iff n \mid r_2 - r_1 \end{aligned}$$

- 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:

$$\begin{cases} -n < r_2 - r_1 < n \\ n \mid r_2 - r_1 \iff \exists b \in \mathbb{Z} \mid r_2 - r_1 = nb \end{cases} \iff r_2 - r_1 = 0 \iff r_2 = r_1$$

- A questo punto, poiché $n > 0$, si ha che:

$$nq_1 + r_1 = nq_2 + r_2 \iff nq_1 + 0 = nq_2 + 0 \iff n(q_1 - q_2) = 0 \iff q_1 = q_2$$

□

3.5 Relazione di Coniugio

Definizione 26: 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:

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

Osservazione 11

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

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

Osservazione 12

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:

$$bhb^{-1} = g \implies h \sim g$$

- **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:

Teorema 4: Principio di induzione

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

$$p_1) \implies p_2)$$

$$p_1), p_2) \implies p_3)$$

...

$$p_1), \dots, p_n) \implies p_{n+1})$$

Esempi:

1. • 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

□

Proposizione 11: Identità binomiale di Newton

Dati $a, b \in \mathbb{R}$ e $n \in \mathbb{N}$, si ha che

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

dove il **coefficiente binomiale** è definito come:

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

Dimostrazione:

- **Caso base:**

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

- **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:

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

□

Elementi di Teoria degli Anelli

4.1 Classi laterali sinistre

Proposizione 12

Sia G un gruppo e sia $H \leq G$ sottogruppo. La seguente relazione è una **relazione di 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:**

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

□

Definizione 27: 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 $x \sim y \iff x^{-1}y \in H$:

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

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

Proposizione 13: Insieme quoziente \mathbb{Z}_n

Dato $I(n) \leq \mathbb{Z}$, si ha che:

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

Dimostrazione:

- Considerando la relazione $a \sim b \iff (-a) + b \in I(n)$ (poiché a^{-1} nell'operazione somma corrisponde a $-a$), otteniamo che:

$$\begin{aligned} a \sim b &\iff -a + b = b - a \in I(n) \iff -a + b = nk, \exists k \in \mathbb{Z} \iff \\ &\iff n \mid b - a \iff a \equiv b \pmod{n} \end{aligned}$$

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

□

Esempio:

- Dato $I(3) \triangleleft \mathbb{Z}$, si ha che: $\mathbb{Z}/I(3) = \{[0], [1], [2]\}$. Difatti, 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 $2 \sim 2 \iff -2 + 2 = 0 = 3 \cdot 0 \in I(3)$
- $3 \in [0]$, poiché $3 \sim 0 \iff -3 + 0 = -3 = 3 \cdot (-1) \in I(3)$
- $4 \in [1]$, poiché $4 \sim 1 \iff -4 + 1 = -3 = 3 \cdot (-1) \in I(3)$
- $5 \in [2]$, poiché $5 \sim 2 \iff -5 + 2 = -3 = 3 \cdot (-1) \in I(3)$
- $6 \in [0]$, poiché $6 \sim 0 \iff -6 + 0 = -6 = 3 \cdot (-2) \in I(3)$
- $7 \in [1]$, poiché $7 \sim 1 \iff -7 + 1 = -6 = 3 \cdot (-2) \in I(3)$
- $8 \in [2]$, poiché $8 \sim 2 \iff -8 + 2 = -6 = 3 \cdot (-2) \in I(3)$
- $9 \in [0]$, poiché $9 \sim 0 \iff -9 + 0 = -9 = 3 \cdot (-3) \in I(3)$
- ...

Osservazione 13

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 $[x] = xH$:

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

□

4.1.1 Teorema di Lagrange**Osservazione 14**

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 $|H| = |xH|$

□

Teorema 5: 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

Proposizione 14: Gruppo quoziente G/H

Dato il gruppo abeliano $(G, +)$ e $H \leq G$, si ha che $(G/H, +)$ 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:**

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

□

Corollario 5: 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 $-1 \equiv 10 \pmod{11}$

Proposizione 15: Anello quoziente G/H

Dato l'anello commutativo A e $I \triangleleft A$, si ha che $(A/I, +, \cdot)$ 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:

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

- 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:**

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

□

Corollario 6: 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

Definizione 28: 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:

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

Definizione 29: 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:**

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

□

Osservazione 15

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 contronominale 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 $a \notin A^*$

□

Definizione 30: Dominio di integrità

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

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

Osservazione 16

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

□

Corollario 7

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

Osservazione 17

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:

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

□

Proposizione 16

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:

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

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

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

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

Dunque si verifica che:

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

□

Corollario 8

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

Definizione 31: 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

Definizione 32: 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**

Osservazione 18

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 $p \mid a \vee p \mid b$

□

Osservazione 19

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:

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

□

Proposizione 17

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

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

□

Proposizione 18: 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

Definizione 33: Dominio ad ideali principali

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

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

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

Proposizione 19

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

Dimostrazione:

- Supponiamo che esista $I \triangleleft \mathbb{Z}$ 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

$$\exists d \in I_{>0} \mid d = \min(I_{>0})$$

- 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:

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

□

Definizione 34: Massimo Comun Divisore (MCD)

Dati $a_1, \dots, a_n \in \mathbb{Z}$, definiamo $d \in \mathbb{N}$ come **massimo comun divisore di** a_1, \dots, a_n , indicato come $d := \text{MCD}(a_1, \dots, a_n)$, se dato $k \in \mathbb{Z}$ si verifica che

$$k \mid a_1 \wedge \dots \wedge k \mid a_n \iff k \mid d$$

Proposizione 20: Identità di Bézout

Dati $a_1, \dots, a_n \in \mathbb{Z}$ e dato $d := \text{MCD}(a_1, \dots, a_n)$, si ha che:

$$I(a_1, \dots, a_n) = I(d)$$

In altre parole, si ha che:

$$\exists x_1, \dots, x_n \in \mathbb{Z} \mid a_1 x_1 + \dots + a_n x_n = d$$

che definiamo come **identità di Bézout**.

Dimostrazione:

- Essendo \mathbb{Z} un dominio ad ideali principali, si ha che

$$\exists n \in I(a_1, \dots, a_n) \mid I(a_1, \dots, a_n) = I(b)$$

- Dato $d := \text{MCD}(a_1, \dots, a_n)$, ovviamente, si ha che

$$d := \text{MCD}(a_1, \dots, a_n) \implies d \mid a_1 \wedge \dots \wedge d \mid a_n \iff \forall i \in [1, n], \exists k_i \in \mathbb{Z} \mid a_i = dk_i$$

- Di conseguenza, otteniamo che

$$b \in I(b) = I(a_1, \dots, a_n) \iff \exists x_1, \dots, x_n \in \mathbb{Z} \mid a_1 x_1 + \dots + a_n x_n = b \iff$$

$$(dk_1)x_1 + \dots + (dk_n)x_n = b \iff d(k_1 x_1 + \dots + k_n x_n) = b \iff d \mid b$$

- Inoltre, $\forall i \in [1, n]$ si ha che

$$a_i \in I(a_i) \subseteq I(a_1, \dots, a_n) = I(b) \iff \exists k \in \mathbb{Z} \mid a_i = bk \iff b \mid a_i$$

- Dunque, per definizione stessa di massimo comun divisore si ha che

$$b \mid a_1 \wedge \dots \wedge b \mid a_n \iff b \mid d$$

- Poiché $d \mid b$, $b \mid d$ e $d \in \mathbb{N}$ necessariamente si ha che $d = b$

□

Proposizione 21

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

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

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 $d := \text{MCD}(a, n) > 0$, 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 $\text{MCD}(a, n) = 1$ si ha che:

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

□

Corollario 9: 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:

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

□

Teorema 6

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

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

Posto $d := \text{MCD}(a, n)$ 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 $d := \text{MCD}(a, n)$, 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 1**

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:

$$z \in I(b, c) \iff z = bx + cy, \exists x, y \in \mathbb{Z} \implies z = (ax)x + (ah)c, \exists k, h \in \mathbb{Z} \implies$$

$$\implies z = a(kx) + a(hc) = a(kx + hc) \implies a \mid z$$

□

Metodo 1: Algoritmo di Euclide

Siano $a, b \in \mathbb{Z}$ e sia $d := \text{MCD}(a, b)$. 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 $r_{i+1} := r_{i-1}(\bmod r_i)$ 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 $\text{MCD}(a, b) = r_n$

Dimostrazione correttezza algoritmo:

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

$$r_2 \equiv r_0(\bmod r_1) \iff r_0 = r_1 q_1 + r_2 \iff r_2 = r_0 - r_1 q_1 \in I(a, b) = I(d)$$

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

Dimostriamo quindi il passo induttivo:

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

- Di conseguenza, $\forall i \in [0, n]$ si ha che

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

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

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

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

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

- Dunque, poiché $r_n, r_{n-1}, r_{n-2} \in I(r_{n-1}, r_n) \subseteq \mathbb{Z}$, per il lemma precedente si ha che:

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

- 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 $d := \text{MCD}(a, b)$ e dati $r_1 := a, r_0 := b$, 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 $\text{MCD}(448, 216)$. 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 $\text{MCD}(448, 216) = 8$

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

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

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

$$216x + 448y = 8$$

A questo punto, riscriviamo il risultato secondo la forma espressa dell'identità di Bézout utilizzando i calcoli dell'algoritmo di Euclide:

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

$$\begin{aligned} - 216 &= 16 \cdot 13 + 8 \implies 8 = 216 - 16 \cdot 13 = 216 - (448 - 216 \cdot 2) \cdot 13 = \\ &= 216 \cdot 27 + 448 \cdot (-13) \end{aligned}$$

Dunque otteniamo che

$$216x + 448y = 8 = 216(27) + 448(-13) \implies x = 27, y = -13$$

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

$$\text{MCD}(a, b, c) = \text{MCD}(a, \text{MCD}(b, c)) = \text{MCD}(\text{MCD}(a, b), c)$$

$$- d := \text{MCD}(b, c) = \text{MCD}(8316, 12600)$$

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

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

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

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

dunque $d = 252$

- A questo punto, riscriviamo il risultato secondo la forma espressa dell'identità di Bézout utilizzando i calcoli dell'algoritmo di Euclide:

$$* 12600 = 8316 \cdot 1 + 4284 \implies 4284 = 12600 - 8316 \cdot 1$$

$$* 8316 = 4284 \cdot 1 + 4032 \implies 4032 = 8316 - 4284 \cdot 1 = 8316 - (12600 - 8316 \cdot 1) = 8316 \cdot 2 - 12600$$

$$* 4284 = 4032 \cdot 1 + 252 \implies 252 = 4284 - 4032 \cdot 1 = (12600 - 8316 \cdot 1) - (8316 \cdot 2 - 12600) = 12600 \cdot 2 - 8316 \cdot 3$$

Dunque otteniamo che

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

$$- p := \text{MCD}(a, d) = \text{MCD}(1470, 252)$$

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

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

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

dunque $p = 42$

- A questo punto, riscriviamo il risultato secondo la forma espressa dell'identità di Bézout utilizzando i calcoli dell'algoritmo di Euclide:

$$* 1470 = 252 \cdot 5 + 210 \implies 210 = 1470 - 252 \cdot 5$$

$$* 252 = 210 \cdot 1 + 42 \implies 42 = 252 - 210 \cdot 1 = 252 - (1470 - 252 \cdot 5) = 1470 \cdot (-1) + 252 \cdot 6$$

Dunque otteniamo che

$$1470z + 252w = 1470(-1) + 252(6) \implies x = -1, y = 6$$

- Infine, ricostruiamo l'identità di Bézout richiesta tramite le due precedentemente calcolate:

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

$$1470x + 8316y + 12600z = 1470 \cdot (-1) + 252 \cdot 6$$

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

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

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

4.5.2 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:

- 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

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

Di conseguenza, possiamo stabilire dei criteri di divisibilità utilizzando le precedenti riduzioni e il fatto che $n \mid m \iff m \equiv 0 \pmod{n}$.

Esempi:

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

$$129383716 \equiv [6 + 1 + 7 + 3 + 8 + 3 + 9 + 2 + 1] \equiv 40 \not\equiv 0 \pmod{3}$$

dunque $3 \nmid 129383716$

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

$$129383716 \equiv [6 - 1 + 7 - 3 + 8 - 3 + 9 - 2 + 1] \equiv 22 \equiv 0 \pmod{11}$$

dunque $11 \mid 129383716$

la definizione stessa di congruenza a 0 in modulo

4.6 Minimo comune multiplo

Definizione 35: Minimo Comune Multiplo (mcm)

Dati $a_1, \dots, a_n \in \mathbb{Z}$, definiamo $m \in \mathbb{N}$ come **minimo comune multiplo di a e b** , indicato come $m := \text{mcm}(a_1, \dots, a_n)$, se dato $k \in \mathbb{Z}$ si verifica che

$$a_1 \mid k \wedge a_n \mid k \iff m \mid k$$

Proposizione 22

Dati $a_1, \dots, a_n \in \mathbb{Z}$ e dato $m := \text{mcm}(a_1, \dots, a_n)$, si ha che:

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

Dimostrazione:

- Essendo \mathbb{Z} un dominio ad ideali principali, si ha che

$$\exists b \in I(a_1, \dots, a_n) \mid I(a_1) \cap \dots \cap I(a_n) = I(b)$$

- Dato $m := \text{mcm}(a_1, \dots, a_n)$, ovviamente, si ha che

$$\begin{aligned} m := \text{mcm}(a_1, \dots, a_n) &\implies a_1 \mid m \wedge a_n \mid m \iff \forall i \in [1, n], \exists k_i \in \mathbb{Z} \mid m = a_i k_i \\ &\iff m \in I(a_i) \iff m \in I(a_1) \cap \dots \cap I(a_n) = I(b) \iff b \mid m \end{aligned}$$

- Inoltre, si ha che

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

- Dunque, per definizione stessa di minimo comune multiplo di ha che

$$a_i \mid b \wedge \dots \wedge a_n \mid b \iff m \mid b$$

- Poiché $m \mid b$, $b \mid m$ e $m \in \mathbb{N}$ necessariamente si ha che $m = b$

□

Osservazione 20

Dato il dominio ad ideali principali \mathbb{Z} e dati $I_1, \dots, I_n \triangleleft A$ 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:

$$\begin{aligned} I_1 + \dots + I_n &= I(a_1) + \dots + I(a_n) = \{b_1 + \dots + b_n \mid b_i \in I(a_i), \forall i \in [0, 1]\} = \\ &= \{b_1 + \dots + b_n \mid b_i = a_i x_i, \exists x_i \in \mathbb{Z}, \forall i \in [0, 1]\} = \{a_1 x_1 + \dots + a_n x_n \mid x_i \in \mathbb{Z}, \forall i \in [0, 1]\} = \\ &= I(a_1, \dots, a_n) = I(d) \end{aligned}$$

dove $d := \text{MCD}(a_1, \dots, a_n)$

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

$$\begin{aligned} x \in I_1 \cdot \dots \cdot I_n &= I(a_1) \cdot \dots \cdot I(a_n) \iff \\ \iff \exists b_{j_{a_i}} \in I(a_i), \forall i, j \in [1, 0] \mid x &= a_1 b_{1_{a_1}} \cdot \dots \cdot a_n b_{1_{a_n}} + \dots + a_1 b_{n_{a_1}} \cdot \dots \cdot a_n b_{n_{a_n}} \iff \\ \iff x &= a_1 \cdot \dots \cdot a_n (b_{1_{a_1}} \cdot \dots \cdot b_{1_{a_n}} + \dots + b_{n_{a_1}} \cdot \dots \cdot b_{n_{a_n}}) \iff x \in I(a_1 \cdot \dots \cdot a_n) \end{aligned}$$

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 $m := \text{mcm}(a_1, \dots, a_n)$

□

Proposizione 23: Infinite soluzioni all'identità di Bézout

Dati $a, n \in \mathbb{Z}$ siano x_0 e y_0 due soluzioni particolari della loro identità di Bézout (es: trovate tramite l'algoritmo di Euclide).

Posti $d := \text{MCD}(a, b)$ e $m := \text{mcm}(a, b)$, tale identità ammette **infinite soluzioni** nella seguente forma:

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

Dimostrazione:

- Prima di tutto, verifichiamo che le soluzioni possibili siano effettivamente valide:

$$a(x_0 + \frac{m}{a}k) + b(y_0 - \frac{m}{b}k) = d \iff ax_0 + mk + by_0 - mk = d \iff ax_0 + by_0 = d$$

- 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 $m := \text{mcm}(a, b)$. Dunque si ha che $\exists k \in \mathbb{Z} \mid N = mk$:

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

□

4.7 Teorema fondamentale dell'aritmetica

Teorema 7: Teorema fondamentale dell'aritmetica

Dato $n \geq 2 \in \mathbb{N}$, tale n può essere espresso come un'unica (a meno di riordinamento) **fattorizzazione in numeri interi primi**, ossia:

$$\exists! p_1, \dots, p_k \in \mathbb{P}, a_1, \dots, a_k \in \mathbb{N}_{>0} \mid n = p_1^{a_1} \cdot \dots \cdot p_k^{a_k}$$

Dimostrazione esistenza:

- Definiamo $S := \{n \in \mathbb{N} \mid n \geq 2 \wedge n \text{ non fattorizzabile in numeri primi}\}$ e supponiamo per assurdo che $|S| \neq 0$. Poiché $S \subseteq \mathbb{N}$, per il principio del buon ordinamento ne segue che $\exists m \in S \mid m = \min(S)$
- Supponiamo quindi che $\exists a, b \neq 0 \in \mathbb{N} - \mathbb{P} \mid m = ab$, da cui traiamo che:

$$\begin{cases} a \mid m \implies a \leq m \\ b \mid m \implies b \leq m \\ m = \min(S) \end{cases} \implies a, b \notin S \implies \begin{cases} a = 1 \vee a \text{ fatt. in primi} \\ b = 1 \vee b \text{ fatt. in primi} \end{cases}$$

- Consideriamo quindi i vari casi:

- Se $a = 1 \wedge b = 1$, allora $m = ab = 1$, contraddicendo l'ipotesi per cui $m \in S \implies m \geq 2$
- Se a fatt. in primi $\wedge b = 1$, allora $m = a = p_1^{a_1} \cdot \dots \cdot p_k^{a_k}$, contraddicendo l'ipotesi per cui $m \in S \implies m$ non fatt. in primi
- Se $a = 1 \wedge b$ fatt. in primi, allora $m = b = q_1^{b_1} \cdot \dots \cdot q_j^{b_j}$, contraddicendo l'ipotesi per cui $m \in S \implies m$ non fatt. in primi
- Se a fatt. in primi $\wedge b$ fatt. in primi, allora

$$m = ab = p_1^{a_1} \cdot \dots \cdot p_k^{a_k} \cdot q_1^{b_1} \cdot \dots \cdot q_j^{b_j}$$

contraddicendo l'ipotesi per cui $m \in S \implies m$ non fatt. in primi

- Di conseguenza, ne segue necessariamente che $|S| = 0$ e dunque che tale fattorizzazione valga $\forall n \geq 2 \in \mathbb{N}$

□

Dimostrazione unicità:

- Dato $n \geq 2 \in \mathbb{N}$, consideriamo le sue due fattorizzazioni:

$$p_1^{a_1} \cdot \dots \cdot p_k^{a_k} = n = q_1^{b_1} \cdot \dots \cdot q_j^{b_j}$$

- Dato che $p_i^{a_i} \mid p_1^{a_1} \cdot \dots \cdot p_k^{a_k}, \forall i \in [1, k]$ e che $p_i \in \mathbb{P}$, ne segue automaticamente che:

$$p_i^{a_i} \mid p_1^{a_1} \cdot \dots \cdot p_k^{a_k} \iff p_i^{a_i} \mid q_1^{b_1} \cdot \dots \cdot q_j^{b_j} \implies$$

$$\implies p_i \mid p_i^{a_i} \wedge p_i^{a_i} \mid q_1^{b_1} \cdot \dots \cdot q_j^{b_j} \implies p_i \mid q_1^{b_1} \cdot \dots \cdot q_j^{b_j} \implies p_i \mid q_1^{b_1} \vee \dots \vee p_i \mid q_j^{b_j}$$

- Sia quindi $q_h \mid h \in [1, j]$ tale che $p_i \mid q_h^{b_h}$. Poiché $q_h \in \mathbb{P}$, ne segue necessariamente che:

$$p_i \mid q_h^{b_h} \implies p_i \mid q_h \implies p_i = q_h$$

dunque concludiamo che $\forall i \in [1, k], \exists h \in [1, j]$ tale che $p_i \mid q_h \implies p_i = q_h \wedge k = j$

□

Proposizione 24: Prodotto tra mcm e MCD

Dati $a, b \in \mathbb{N}$, si ha che:

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

Dimostrazione:

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

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

- Se invece $a = b = 1$, allora:

$$\text{mcm}(a, b) \cdot \text{MCD}(a, b) = 1 \cdot 1 = 1 = ab$$

- Supponiamo quindi che $a, b \geq 2$. Per il teorema fondamentale dell'aritmetica, a e b sono esprimibili come una fattorizzazione in numeri interi primi. Poniamo quindi:

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

dove $p \nmid a \implies a_p = 0$ e $p \nmid b \implies b_p = 0$ (ossia tale numero intero primo non compare nella loro fattorizzazione)

- Poniamo inoltre $d := \text{MCD}(a, b)$ e $m := \text{mcm}(a, b)$, 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:

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

□

Osservazione 21

Dati $a_1, \dots, a_n \in \mathbb{N}$ dove $n > 2 \in \mathbb{N}$, non è detto che:

$$\text{mcm}(a_1, \dots, a_n) \cdot \text{MCD}(a_1, \dots, a_n) = a_1 \cdot \dots \cdot a_n$$

4.8 Teorema cinese dei resti

Lemma 2: Numeri coprimi ed mcm

Dati $a_1, \dots, a_n \geq 2 \in \mathbb{N}$, si ha che:

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

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

Dimostrazione:

- Dati $a_1, \dots, a_n \geq 2 \in \mathbb{N}$, per il teorema fondamentale dell'aritmetica si ha che:

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

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

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

- Di conseguenza, per ogni esponente $a_{i,p} > 0$ si ha che $a_{j,p} = 0, \forall j \neq i$, da cui ne segue che:

$$\forall p \in \mathbb{P}, \exists! a_{k,p} > 0 \mid a_{1,p} + \dots + a_{n,p} = a_{k,p} = \max(a_{1,p}, \dots, a_{n,p})$$

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

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

□

Lemma 3

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

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

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

Dimostrazione:

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

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

□

Teorema 8: Teorema cinese dei resti

Dati $a_1, \dots, a_n \geq 2 \in \mathbb{N}$ **coprimi tra loro**, dunque tali che $\text{MCD}(a_i, a_j) = 1, \forall i \neq j$ 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

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

dove $m := \text{mcm}(a_1, \dots, a_n) = a_1 \cdot \dots \cdot a_n$ 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 $m := \text{mcm}(a_1, \dots, a_n)$, per il lemma precedente si ha che:

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

- 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.
- Poiché φ è biettiva, 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:

1. • 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 $[a] = [2] \in \mathbb{Z}_5 \iff a \equiv 2 \pmod{5} \iff a = 2 + 5b, \exists b \in \mathbb{Z}$
- Sostituendo $x = 2 + 3(2 + 5b) = 8 + 15b$ dentro $x \equiv 2 \pmod{7}$, otteniamo che:

$$8 + 15b \equiv 2 \pmod{5}$$

- 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 $[b] = [1] \in \mathbb{Z}_7 \iff b \equiv 1 \pmod{7} \iff b = 1 + 7c, \exists c \in \mathbb{Z}$
- Infine, otteniamo che

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

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

$$\begin{cases} 23 \equiv 2 \pmod{3} \\ 23 \equiv 3 \pmod{5} \\ 23 \equiv 2 \pmod{7} \end{cases}$$

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 $x = 3(2 + 5b) = 6 + 15b \iff 6 + 15b \equiv 3(\text{mod } 4)$. Lavorando in \mathbb{Z}_4 si ha che:

$$[6 + 15b] = [3] \iff [6] + [15][b] = [3] \iff$$

$$\iff [2] + [3][b] = [3] \iff [3][b] = [3] - [2] \iff$$

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

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

$$[51 + 60c] = [1] \iff [2] + [4][c] = [1] \iff [2] + [4][c] = [1] \iff$$

$$\iff [4][c] = [1] - [2] \iff [4][c] = [-1] \iff [c] = [6][4]^{-1} \iff$$

$$\iff [c] = [6][2] \iff [c] = [12] \iff [c] = [5]$$

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

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

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

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

4. • Vogliamo calcolare le ultime due cifre di 37^{37} . Poniamo quindi $x := 37^{37}$ e calcoliamo la classe di equivalenza $x \bmod 100$.
- 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:

$$\begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 17 \pmod{25} \end{cases}$$

- Abbiamo quindi che $x = 1 + 4k \implies 1 + 4k \equiv 17 \pmod{25}$:

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

- Dunque $k \equiv 4 \pmod{25} \implies k = 4 + 25j \implies x = 1 + 4(4 + 25j) = 17 + 100j$
- Quindi concludiamo che $x \equiv 17 \pmod{100}$ 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 $193x \equiv 1 \pmod{240}$
- Dato che $240 = 3 \cdot 5 \cdot 16$, applichiamo il teorema cinese dei resti

$$193x \equiv 1 \pmod{240} \iff \begin{cases} 193x \equiv 1 \pmod{3} \\ 193x \equiv 1 \pmod{5} \\ 193x \equiv 1 \pmod{16} \end{cases}$$

- Riduciamo le classi di equivalenza del sistema:

– Riduciamo $193x \equiv 1 \pmod{3}$ in:

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

- Riduciamo $193x \equiv 1 \pmod{5}$ in:

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

- Riduciamo $193x \equiv 1 \pmod{16}$ 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 dei resti:

$$\begin{cases} 193x \equiv 1 \pmod{3} \\ 193x \equiv 1 \pmod{5} \\ 193x \equiv 1 \pmod{16} \end{cases} \implies \begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 1 \pmod{16} \end{cases}$$

- 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 $[193][97] = [1]$

Proposizione 25

Dati $n, m \in \mathbb{Z}$ tali che $m \mid n$, si ha che:

$$x \equiv y \pmod{n} \implies x \equiv y \pmod{m}$$

Dimostrazione:

- Poiché $m \mid n \iff n = mk, k \in \mathbb{Z}$, il risultato segue automaticamente dalla definizione di congruenza:

$$x \equiv y \pmod{n} \iff x = y + nh, h \in \mathbb{Z} \implies x = y + mkh \iff x \equiv y \pmod{m}$$

□

Esempi:

- Consideriamo il seguente sistema:

$$\begin{cases} x \equiv 2 \pmod{12} \\ x \equiv 4 \pmod{8} \end{cases}$$

- Applicando il teorema cinese dei resti otteniamo che

$$\begin{cases} x \equiv 2(\text{mod } 12) \\ x \equiv 4(\text{mod } 8) \end{cases} \iff \begin{cases} x \equiv 2(\text{mod } 3) \\ x \equiv 2(\text{mod } 4) \\ x \equiv 4(\text{mod } 8) \end{cases}$$

- Poiché $4 \mid 8$, per la proposizione precedente si ha che:

$$x \equiv 4(\text{mod } 8) \implies x \equiv 4 \equiv 0(\text{mod } 4)$$

- Di conseguenza, il sistema risulta incompatibile poiché

$$x \equiv 2(\text{mod } 4) \iff x \not\equiv 0(\text{mod } 4)$$

2. • Consideriamo il seguente sistema:

$$\begin{cases} x \equiv 0(\text{mod } 12) \\ x \equiv 4(\text{mod } 8) \end{cases}$$

- Applicando il teorema cinese dei resti otteniamo che

$$\begin{cases} x \equiv 0(\text{mod } 12) \\ x \equiv 4(\text{mod } 8) \end{cases} \iff \begin{cases} x \equiv 0(\text{mod } 3) \\ x \equiv 0(\text{mod } 4) \\ x \equiv 4(\text{mod } 8) \end{cases}$$

- Poiché $4 \mid 8$, per la proposizione precedente si ha che:

$$x \equiv 4(\text{mod } 8) \implies x \equiv 4 \equiv 0(\text{mod } 4)$$

- Di conseguenza, il sistema risulta compatibile, implicando che esso possa essere ridotto in

$$\begin{cases} x \equiv 0(\text{mod } 12) \\ x \equiv 4(\text{mod } 8) \end{cases} \iff \begin{cases} x \equiv 0(\text{mod } 3) \\ x \equiv 0(\text{mod } 4) \\ x \equiv 4(\text{mod } 8) \end{cases} \iff \begin{cases} x \equiv 0(\text{mod } 3) \\ x \equiv 4(\text{mod } 8) \end{cases}$$

4.9 Piccolo teorema di Fermat

Lemma 4

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 $\frac{(p-1)!}{k! \cdot (p-k)!} \in \mathbb{Z}$ poiché per definizione di coefficiente binomiale si ha che $\binom{p}{k} \in \mathbb{N}$

□

Esempio:

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

Corollario 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 5

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 $[0]$:

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

□

Corollario 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:

$$\begin{aligned} ([a_1] + \dots + [a_n] + [a_{n+1}])^p &= (([a_1] + \dots + [a_n]) + [a_{n+1}])^p = \\ &= ([a_1] + \dots + [a_n])^p + [a_{n+1}]^p = [a_1]^p + \dots + [a_n]^p + [a_{n+1}]^p \end{aligned}$$

□

Teorema 9: 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:

$$[a+1]^p = ([a]+[1])^p = [a]^p + [1]^p = [a]^p + [1] = [a] + [1] = [a+1]$$

□

Corollario 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:

$$\begin{aligned} 4^{-1} &\equiv 4^{13-2} \pmod{13} \iff [4]^{-1} = [4]^{11} = [4][4]^{10} = [4][4^2]^5 = [4][16]^5 = \\ &= [4][3]^5 = [4][3]^2[3]^3 = [4][9][27] = [4][9][1] = [36] = [10] \end{aligned}$$

4.10 Funzione totiente di Eulero

Definizione 36: Funzione totiente di Eulero

Dato $n \in \mathbb{N}$, definiamo come $\varphi(n)$ come **funzione totiente di Eulero**, dove:

$$\varphi : \mathbb{N} \rightarrow \mathbb{N} : n \mapsto |\mathbb{Z}_n^*|$$

Lemma 6

Dati i due anelli commutativi \mathbb{Z}_m e \mathbb{Z}_n , dove $\text{MCD}(m, n) = 1$, si ha che:

$$[a] \in \mathbb{Z}_{mn}^* \iff [a] \in \mathbb{Z}_m^*, [a] \in \mathbb{Z}_n^*$$

Dimostrazione:

- Supponiamo che $[a] \in \mathbb{Z}_{mn}^*$, da cui ricaviamo che:

$$[a] \in \mathbb{Z}_{mn}^* \iff \exists x \in \mathbb{Z}_{mn} \mid ax \equiv 1(\text{mod } mn)$$

- Poiché $\text{MCD}(m, n) = 1 \implies \text{mcm}(m, n) = mn$, per il teorema cinese dei resti si ha che:

$$ax \equiv 1(\text{mod } mn) \iff \begin{cases} ax \equiv 1(\text{mod } m) \\ ax \equiv 1(\text{mod } n) \end{cases} \iff [a] \in \mathbb{Z}_m^*, [a] \in \mathbb{Z}_n^*$$

□

Osservazione 22

Dati $m, n \in \mathbb{N}$ dove $\text{MCD}(m, n) = 1$, si ha che:

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Dimostrazione:

- Per il lemma precedente, la seguente funzione $f : \mathbb{Z}_{mn}^* \rightarrow \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ risulta essere biettiva, implicando che:

$$\varphi(mn) = |\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^* \times \mathbb{Z}_n^*| = |\mathbb{Z}_m^*| \cdot |\mathbb{Z}_n^*| = \varphi(m)\varphi(n)$$

□

Osservazione 23

Dati $p \in \mathbb{P}$ e $k \neq 0 \in \mathbb{N}$, si ha che:

$$\varphi(p^k) = p^{k-1}(p-1)$$

Dimostrazione:

- Per dimostrazione precedente, per ogni $0 < a < p^k$, si ha che:

$$[a] \in \mathbb{Z}_{p^k}^* \iff \text{MCD}(a, p^k) = 1$$

- Inoltre, poiché $p \in \mathbb{P}$, si ha che:

$$\text{MCD}(a, p^k) = 1 \iff p \nmid a \iff \nexists n \in \mathbb{Z} \mid a = np$$

- Simmetricamente, quindi, si ha che:

$$[a] \notin \mathbb{Z}_{p^k}^* \iff \text{MCD}(a, p^k) \neq 1 \iff p \mid a \iff \exists n \in \mathbb{Z} \mid a = np$$

- Consideriamo quindi i multipli di p compresi tra 0 e p^k (escluso):

$$0 \leq np < p^k \implies 0 \leq n \leq p^{k-1}$$

da cui traiamo che la cardinalità degli elementi non invertibili in \mathbb{Z}_{p^k} corrisponde a:

$$H := \{[a] \in \mathbb{Z}_{p^k} \mid [a] \notin \mathbb{Z}_{p^k}^*\} \implies |H| = p^{k-1}$$

- Infine, quindi, concludiamo che:

$$\varphi(p^k) = |\mathbb{Z}_{p^k}| - |H| = p^k - p^{k-1} = p^{k-1}(p - 1)$$

□

Proposizione 26

Dato $n \geq 2 \in \mathbb{N}$, si ha che:

$$\varphi(n) = n \prod_{\substack{p \in \mathbb{P} \\ \text{t.c. } p \mid n}} \left(1 - \frac{1}{p}\right)$$

Dimostrazione:

- Per il teorema fondamentale dell'aritmetica si ha che:

$$\exists! p_1, \dots, p_k \in \mathbb{P}, i_1, \dots, i_k \in \mathbb{N}_{>0} \mid n = p_1^{i_1} \cdot \dots \cdot p_k^{i_k}$$

- Poiché tali fattori sono tutti coprimi tra loro, si ha che:

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{i_1}) \cdot \dots \cdot \varphi(p_k^{i_k}) = p_1^{i_1-1}(p_1 - 1) \cdot \dots \cdot p_k^{i_k-1}(p_k - 1) = \\ &= \frac{p_1^{i_1}(p_1 - 1)}{p_1} \cdot \dots \cdot \frac{p_k^{i_k}(p_k - 1)}{p_k} = n \prod_{\substack{p \in \mathbb{P} \\ \text{t.c. } p \mid n}} \left(1 - \frac{1}{p}\right) \end{aligned}$$

□

4.11 Ordine di un elemento di un gruppo

Definizione 37: 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** $I(g) \triangleleft \mathbb{Z}$ come:

$$H(g) := \{g^n \mid n \in \mathbb{Z}\}$$

$$I(g) := \{n \in \mathbb{Z} \mid g^n = e\}$$

Dimostrazioni:

- $H \leq G$
 - $g^0 = e \implies e \in H(g)$
 - $g^n, g^m \in H(g) \implies g^n \cdot g^m = g^{n+m} \implies g^{n+m} \in H(g)$
 - $g^n \in H(g) \implies (g^n)^{-1} = g^{-n} \implies g^{-n} \in H(g)$
- $I(g) \triangleleft \mathbb{Z}$
 - $g^0 = e \implies 0 \in I(g)$
 - $n, m \in I(g) \implies g^n = g^m = e \implies g^{n+m} = g^n \cdot g^m = e \implies n+m \in I(g)$
 - $n \in I(g) \implies g^{-n} = (g^n)^{-1} = e^{-1} = e \implies -n \in I(g)$
 - $n \in I(g), k \in \mathbb{Z} \implies g^{nk} = (g^n)^k = e^k = e \implies kn \in I(g)$

□

Definizione 38: Ordine di un elemento

Sia G un gruppo. Dato $g \in G$, definiamo l'**ordine di g** come:

$$o(g) := |H(g)|$$

Proposizione 27

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 $I(g) \triangleleft \mathbb{Z}$ 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 $\forall n \in \mathbb{Z}, \exists r \in [0, d) \mid g^n = g^r$ 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 $g(x) = g^x \in H(g), \forall 0 \leq x < d$:

$$H(g) = \{g^0, \dots, g^{d-1}\}$$

□

Osservazione 24

Sia G un gruppo. Dato $g \in G \mid o(g) < +\infty$ e dato $k \in \mathbb{Z}$, si ha che:

$$g^k = e \implies o(g) \mid k$$

Dimostrazione:

- Sia $d := o(g)$. Dalla definizione stessa di $I(d)$, si ha che:

$$g^k = e \implies k \in I(d) \implies k = dn, n \in \mathbb{Z} \implies d \mid k$$

□

Corollario 13

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 $d := o(g) := |H(g)| \leq |G| < +\infty$, per il teorema di Lagrange si ha che:

$$o(g) \mid |G| \implies d \mid |G| \implies |G| = dk, \exists k \in \mathbb{Z} \implies g^{|G|} = g^{dk} = (g^d)^k = e^k = e$$

□

Corollario 14: Piccolo teorema di Fermat (II dim.)

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:

$$o(a) \mid |\mathbb{Z}_p^*| \implies [a]^{|\mathbb{Z}_p^*|} = [1] \implies [a]^{p-1} = [1] \implies [a]^p [a]^{-1} = [1] \implies [a]^p = [a]$$

□

Teorema 10: Teorema di Eulero

Dati $a, n \in \mathbb{N}$ tali che $\text{MCD}(a, n) = 1$, si ha che:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

dove $\varphi(n)$ è la funzione totiente di Eulero

Dimostrazione:

- Per dimostrazione precedente, si ha che:

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

- Di conseguenza, si ha che:

$$o(a) \mid |\mathbb{Z}_n^*| \implies [a]^{|\mathbb{Z}_n^*|} = [1] \implies [a]^{\varphi(n)} = [1]$$

□

Proposizione 28: 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

$$|H(g)| = |G| \iff H(g) = G$$

□

Corollario 15

Sia G un gruppo. Dato $g \in G$, si ha che:

$$g \in G^* \implies g^{o(g)-1} = g^{-1}$$

Dimostrazione:

- Siccome $g \in \mathbb{G}^* \iff \exists g^{-1} \in \mathbb{G}$, allora:

$$g^{o(g)} = 1 \iff g^{o(g)} g^{-1} = g^{-1} \iff g^{o(g)-1} = g^{-1}$$

□

Lemma 7

Sia G un gruppo. Dato $g \in G$, si ha che:

$$g \in G^* \implies o(g) = o(g^{-1})$$

Dimostrazione:

- Siccome $g \in \mathbb{G}^* \iff \exists g^{-1} \in \mathbb{G}$, 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 8

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 $H(g^k) \leq H(g)$

$$- (g^k)^n \in H(g^k) \implies (g^k)^n = g^{kn} \in H(g) \implies H(g^k) \subseteq H(g)$$

$$- (g^k)^0 = g^0 = e \in H(g^k)$$

$$- (g^k)^n, (g^k)^m \in H(g) \implies (g^k)^n (g^k)^m = g^{kn} g^{km} = g^{kn+km} = g^{k(n+m)} = (g^k)^{n+m} \in H(g)$$

$$- (g^k)^n \in H(g^k) \implies ((g^k)^n)^{-1} = (g^k)^{-n} \in H(g^k)$$

- Di conseguenza, per il teorema di Lagrange si ha che

$$|H(g^k)| \mid |H(g)| \iff o(g^k) \mid o(g)$$

□

Lemma 9

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 $m := \text{mcm}(o(g), o(h))$ e $d := \text{MCD}(o(g), o(h))$.

In particolare, se $d = 1$, allora $o(gh) = o(g)o(h)$.

Dimostrazione:

- Per definizione stessa di $m := \text{mcm}(o(g), o(h))$, 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 $d = \text{MCD}(o(g), o(h))$

- 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:

$$o(gh) = m = o(g)o(h)$$

□

Proposizione 29

Siano $n_1, \dots, n_k \neq 0 \in \mathbb{N} \mid \text{MCD}(a_i, a_j) \iff i \neq j$ e sia $N := \text{mcm}(n_1, \dots, n_k) = n_1 \cdot \dots \cdot n_k$.

Dato $[a] \in \mathbb{Z}_m^*$, dove $m := \text{mcm}(o_1, \dots, o_k)$ e dove $o_h := o([a])$ nel gruppo $\mathbb{Z}_{n_h}^*, \forall 0 < h < k$, posto $o := o([a])$ nel gruppo \mathbb{Z}_m^* si ha che:

$$o = m := \text{mcm}(o_1, \dots, o_k)$$

Dimostrazione:

- Per il teorema cinese dei resti, abbiamo che:

$$\begin{aligned} a^o \equiv 1 \pmod{N} &\iff \begin{cases} a^o \equiv 1 \pmod{n_1} \\ \vdots \\ a^o \equiv 1 \pmod{n_k} \end{cases} \iff \\ &\iff \begin{cases} o_1 \mid o \\ \vdots \\ o_k \mid o \end{cases} \iff m := \text{mcm}(o_1, \dots, o_k) \mid o \end{aligned}$$

- Inoltre, poiché $m := \text{mcm}(o_1, \dots, o_k)$, 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:

$$o \mid m, m \mid o \iff o = m$$

□

Proposizione 30

Dato l'anello commutativo \mathbb{Z}_n , dove $n > 2$, si ha che $o(n-1) = 2$

Dimostrazione:

- Dalle proprietà dei moduli ne segue direttamente che:

$$(n-1)^2 \equiv n^2 - 2n + 1 \equiv 0^2 - 2 \cdot 0 + 1 \equiv 1 \pmod{n}$$

- Di conseguenza, otteniamo che:

$$2 = o(n-1)k, k \in \mathbb{Z} \implies o(n-1) \mid 2 \implies o(n-1) \in \{1, 2\}$$

- Poiché $(n-1)^1 \equiv n-1 \pmod{n}$ e $n > 2 \implies n-1 > 1$, ne segue necessariamente che $n-1 \not\equiv 1 \pmod{n}$ e di conseguenza che $o(n-1) \neq 1$.
- Dunque, l'unica possibilità è che $o(n-1) = 2$

□

Corollario 16

Dato l'anello commutativo \mathbb{Z}_n , dove $n > 2$, si ha che $|\mathbb{Z}_n^*| = 2k, k \in \mathbb{N}$, ossia che $|\mathbb{Z}_n^*|$ è sempre pari

Dimostrazione:

- Per la proposizione precedente e il teorema di Lagrange, ne segue automaticamente che

$$o(n-1) = 2 \wedge o(n-1) \mid |\mathbb{Z}_n^*| \implies 2 \mid |\mathbb{Z}_n^*| \implies |\mathbb{Z}_n^*| = 2k, k \in \mathbb{Z}$$

- Poiché la cardinalità di un gruppo non può essere negativa, ne segue necessariamente che $|\mathbb{Z}_n^*| = 2k, k \in \mathbb{N}$

□

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 $g \in \mathbb{Z}_{21}^* \iff \text{MCD}(a, 21) = 1$ (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:

$$o(g) \mid |\mathbb{Z}_{21}^*| \implies o(g) \mid 12 \implies o(g) \in \{1, 2, 3, 4, 6, 12\}$$

- Ricordando che $g^{-1} = g^{o(g)-1}$ e che $o(g) = o(g^{-1})$, calcoliamo gli ordini dei vari invertibili in \mathbb{Z}_{21} trovati:

$$- [1]^1 = 1 \implies \begin{cases} o([1]) = 1 \\ [1]^{-1} = [1]^0 = [1] \end{cases}$$

$$- [2]^6 = [64] = [1] \implies \begin{cases} o([2]) = 6 \\ [2]^{-1} = [2]^5 = [11] \end{cases} \implies \begin{cases} o([11]) = 6 \\ [11]^{-1} = [2] \end{cases}$$

$$- [4]^3 = [2]^6 = [64] = [1] \implies \begin{cases} o([4]) = 3 \\ [4]^{-1} = [4]^2 = [16] \end{cases} \implies \begin{cases} o([16]) = 3 \\ [16]^{-1} = [4] \end{cases}$$

$$- [5]^6 = [5^2]^3 = [4]^3 = [1] \implies \begin{cases} o([5]) = 6 \\ [5]^{-1} = [5]^5 = [17] \end{cases} \implies \begin{cases} o([17]) = 6 \\ [17]^{-1} = [5] \end{cases}$$

$$- [8]^2 = [2]^6 = [1] \implies \begin{cases} o([8]) = 2 \\ [8]^{-1} = [8] \end{cases}$$

$$- [10]^6 = [10^3]^2 = [13]^2 = [1] \implies \begin{cases} o([10]) = 6 \\ [10]^{-1} = [10]^5 = [19] \end{cases} \implies \begin{cases} o([19]) = 6 \\ [19]^{-1} = [10] \end{cases}$$

$$- [13]^2 = [1] \implies \begin{cases} o([13]) = 2 \\ [13]^{-1} = [13]^1 = [13] \end{cases}$$

$$- [20]^2 = [1] \implies \begin{cases} o([20]) = 2 \\ [20]^{-1} = [20]^1 = [20] \end{cases}$$

- Poiché $\nexists g \in \mathbb{Z}_{21}^* \mid o(g) = |\mathbb{Z}_{21}^*| = 12$, concludiamo che \mathbb{Z}_{21}^* non è un gruppo ciclico

5

Gruppo Simmetrico

Osservazione 25

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

□

Definizione 39: 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

$$\forall f \in \mathcal{S}_X, \exists f^{-1} \in \mathcal{S}_X \mid f \circ f^{-1} = f^{-1} \circ f = \text{id}$$

□

Osservazione 26

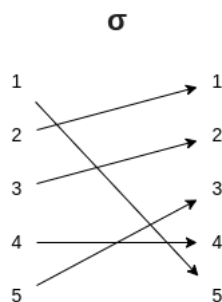
Dato il gruppo simmetrico \mathcal{S}_X , ogni $f \in \mathcal{S}_X$ corrisponde ad una **permutazione** del dominio X , poiché $f : X \rightarrow X$ è biettiva. Dunque, è possibile definire impropriamente \mathcal{S}_X come il "**gruppo delle permutazioni di X** ".

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

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$$

Osservazione 27

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 $\sigma\tau := \sigma \circ \tau = \sigma(\tau(x)), \forall x$.

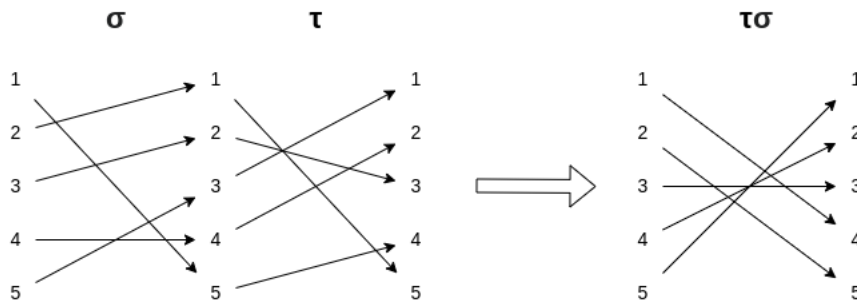
Ovviamente, (\mathcal{S}_n, \cdot) risulta essere un **gruppo** (non abeliano poiché per natura stessa della composizione si ha che $\sigma\tau \neq \tau\sigma$)

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**.

$$\begin{array}{l} \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} \\ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix} \end{array} \Rightarrow \begin{array}{l} \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} \\ \tau = \begin{pmatrix} 5 & 1 & 2 & 4 & 3 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix} \end{array} \Rightarrow \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix}$$

5.1 Ordine di una permutazione

Definizione 40: 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 (1527)
 - $3 \rightarrow 6 \rightarrow 3$ che abbreviamo come (36)
 - $4 \rightarrow 9 \rightarrow 8 \rightarrow 4$ che abbreviamo come (498)

Definizione 41: 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:

$$\tau \in \mathcal{S}_8 \mid \tau = (235)(1874)(6) \implies \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 5 & 1 & 2 & 6 & 4 & 7 \end{pmatrix}$$

Definizione 42

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 $\text{id} = (1)(2) \dots (n-1)(n)$
- $(I(\sigma(i)), +) \triangleleft (\mathbb{Z}, +)$
- $(I(\sigma), +) \triangleleft (\mathbb{Z}, +)$

Dimostrazione:

- $I(\sigma, i) \triangleleft \mathbb{Z}$:
 - $\sigma^0(i) = \text{id}(i) = i \implies 0 \in I(\sigma, i)$
 - $m, n \in I(\sigma, i) \implies \sigma^n(i) = i = \sigma^m(i) \implies \sigma^{n+m}(i) = \sigma^n(\sigma^m(i)) = \sigma^n(i) = i \implies m+n \in I(\sigma, i)$
 - $n \in I(\sigma, i) \implies \sigma^{-n}(i) = (\sigma^n)^{-1}(i) = i \implies -n \in I(\sigma, i)$
 - $n \in I(\sigma, i) \implies \sigma^{nk}(i) = (\sigma^n)^k(i) = i, \forall k \in \mathbb{Z} \implies nk \in I(\sigma, i), \forall k \in \mathbb{Z}$
 - 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 $I(\sigma) \triangleleft \mathbb{Z}$ poiché analoga a quella di $I(\sigma, i) \triangleleft \mathbb{Z}$

□

Lemma 10

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 $I(\sigma, i) \triangleleft \mathbb{Z}$, 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 $h = d_j$

□

Proposizione 31: 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 $I(\sigma) \triangleleft \mathbb{Z}$, 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:

$$o(\sigma) = \text{mcm}(5, 2, 4, 1, 3) = 60$$

5.2 Segno delle permutazioni

Definizione 43: Segno di una permutazione

Sia $\sigma \in \mathcal{S}_n$. Definiamo il **segno di** σ come:

$$\text{sgn}(\sigma) = (-1)^{|\text{inv}(\sigma)|} = \begin{cases} +1 & \text{se } |\text{inv}(\sigma)| \text{ è pari} \\ -1 & \text{se } |\text{inv}(\sigma)| \text{ è dispari} \end{cases}$$

Dove $\text{inv}(\sigma)$ è l'**insieme delle sue inversioni**:

$$\text{inv}(\sigma) := \{(i, j) \mid 1 \leq i < j \leq n, \sigma(i) > \sigma(j)\}$$

Definiamo σ come **pari** se $\text{sgn}(\sigma) = +1$, mentre come **dispari** $\text{sgn}(\sigma) = -1$

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:

$$\text{inv}(\sigma) := \{(1, 4), (2, 3), (2, 4), (2, 5), (3, 4)\}$$

da cui otteniamo che $\text{sgn}(\sigma) = -1$

Definizione 44: 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 11

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 $\sigma \in \mathcal{S}_3$ 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:

$$\begin{aligned} \sigma(\tau_{3,4}\tau_{2,3}\tau_{1,2}\tau_{3,4}) &= \text{id} \iff \\ \iff \sigma(\tau_{3,4}\tau_{2,3}\tau_{1,2}\tau_{3,4})(\tau_{3,4}\tau_{2,3}\tau_{1,2}\tau_{3,4})^{-1} &= \text{id}(\tau_{3,4}\tau_{2,3}\tau_{1,2}\tau_{3,4})^{-1} \iff \\ \iff \sigma &= (\tau_{3,4}\tau_{2,3}\tau_{1,2}\tau_{3,4})^{-1} \iff \sigma = \tau_{3,4}\tau_{1,2}\tau_{2,3}\tau_{3,4} \end{aligned}$$

□

Proposizione 32

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:

$$\begin{aligned} 1 = \text{sgn}(\text{id}) &= \text{sgn}(\sigma(\tau_1 \cdot \tau_2 \cdot \tau_3 \cdot \dots \cdot \tau_k)^{-1}) = \text{sgn}(\sigma \cdot \tau_k \cdot \dots \cdot \tau_3 \cdot \tau_2 \cdot \tau_1) = \\ &= -\text{sgn}(\sigma \cdot \tau_k \cdot \dots \cdot \tau_3 \cdot \tau_2) = \text{sgn}(\sigma \cdot \tau_k \cdot \dots \cdot \tau_3) = \dots = (-1)^k \cdot \text{sgn}(\sigma) \end{aligned}$$

- Quindi, otteniamo che:

$$1 = (-1)^k \cdot \text{sgn}(\sigma) \implies \text{sgn}(\sigma) = (-1)^k$$

□

Corollario 17

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 $\sigma' = \tau'_1 \cdot \dots \cdot \tau'_j$, si ha che:

$$\text{sgn}(\sigma\sigma') = \text{sgn}(\tau_1 \cdot \dots \cdot \tau_k \cdot \tau'_1 \cdot \dots \cdot \tau'_j) = (-1)^{k+j} = (-1)^k (-1)^j = \text{sgn}(\sigma) \cdot \text{sgn}(\sigma')$$

□

Corollario 18

Data $\sigma \in \mathcal{S}_n$, si verifica che:

$$\text{sgn}(\sigma^{-1}) = \text{sgn}(\sigma)$$

Dimostrazione:

$$\begin{aligned} 1 = \text{sgn}(\text{id}) &= \text{sgn}(\sigma\sigma^{-1}) = \text{sgn}(\sigma) \cdot \text{sgn}(\sigma^{-1}) \implies \\ \implies 1 &= \text{sgn}(\sigma) \cdot \text{sgn}(\sigma^{-1}) \iff \text{sgn}(\sigma) = \pm 1 = \text{sgn}(\sigma^{-1}) \end{aligned}$$

□

Definizione 45

Dato il gruppo \mathcal{S}_n , definiamo $\mathcal{A}_n \leq \mathcal{S}_n$ come il **sottogruppo alterno di ordine n** :

$$\mathcal{A}_n := \{\sigma \in \mathcal{S}_n \mid \text{sgn}(\sigma) = +1\}$$

Dimostrazione:

- $\text{sgn}(\text{id}) = 1 \implies \text{id} \in \mathcal{A}_n$

- $\sigma, \tau \in \mathcal{A}_n \implies \text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau) = 1 \cdot 1 = 1 \implies \sigma\tau \in \mathcal{A}_n$
- $\sigma \in \mathcal{A}_n \implies \text{sgn}(\sigma^{-1}) = \text{sgn}(\sigma) = 1 \implies \sigma^{-1} \in \mathcal{A}_n$

□

Osservazione 28

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:

$$\begin{aligned} \sigma \sim \sigma' &\iff \sigma^{-1}\sigma' \in \mathcal{A}_n \iff \text{sgn}(\sigma^{-1}\sigma') = 1 \iff \\ &\iff \text{sgn}(\sigma^{-1})\text{sgn}(\sigma') = 1 \iff \text{sgn}(\sigma) = \text{sgn}(\sigma') \end{aligned}$$

- 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:

$$|\mathcal{A}_n| = \frac{|\mathcal{S}_n|}{[\mathcal{S}_n : \mathcal{A}_n]} = \frac{n!}{2}$$

□

Proposizione 33

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:

$$\begin{aligned} \sigma'(i_q) = \alpha\sigma\alpha^{-1}(i_q) &\iff \sigma'\alpha(i_q) = \alpha\sigma\alpha^{-1}\alpha(i_q) \iff \sigma'\alpha(i_q) = \alpha\sigma(i_q) \implies \\ &\implies \sigma'\alpha(i_q) = \alpha\sigma(i_q) = \begin{cases} \alpha(i_{q+1}) & \text{se } q < d \\ \alpha(i_1) & \text{se } q = d \end{cases} \end{aligned}$$

- 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:

$$\begin{array}{ccccccc} \sigma = & (i_1 & \dots & i_{d_1}) & \dots & (j_1 & \dots & j_{d_k}) \\ & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \sigma' = & (a_1 & \dots & a_{d_1}) & \dots & (b_1 & \dots & b_{d_k}) \end{array}$$

- 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 $\sigma' = \alpha\sigma\alpha^{-1}$:

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 1 & 4 & 2 & 7 & 5 \end{pmatrix} = (4)(13)(2675) \\ \sigma' &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 6 & 5 & 7 \end{pmatrix} = (7)(56)(1234) \end{aligned} \implies \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 6 & 7 & 4 & 2 & 3 \end{pmatrix}$$

Osservazione 29

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

$$\exists \alpha \in \mathbb{S}_n \mid \sigma' = \alpha \sigma \alpha^{-1} \implies \text{sgn}(\sigma') = \text{sgn}(\alpha \sigma \alpha^{-1}) = \text{sgn}(\alpha) \text{sgn}(\sigma) \text{sgn}(\alpha^{-1})$$

- Dunque, poiché $\text{sgn}(\alpha) = \text{sgn}(\alpha^{-1}) = \pm 1 \implies \text{sgn}(\alpha) \text{sgn}(\alpha^{-1}) = 1$, se segue che:

$$\begin{aligned} \text{sgn}(\sigma') &= \text{sgn}(\alpha) \text{sgn}(\sigma) \text{sgn}(\alpha^{-1}) \implies \\ \implies \text{sgn}(\sigma') &= \begin{cases} 1 \cdot \text{sgn}(\sigma) \cdot 1 = \text{sgn}(\sigma) & \text{se } \text{sgn}(\alpha) = 1 \\ (-1) \cdot \text{sgn}(\sigma) \cdot (-1) = \text{sgn}(\sigma) & \text{se } \text{sgn}(\alpha) = -1 \end{cases} \implies \\ &\implies \text{sgn}(\sigma') = \text{sgn}(\sigma) \end{aligned}$$

□

Proposizione 34

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 $\sigma \in \mathbb{S}_n$ 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:

$$\begin{aligned} \sigma' &= (1, \dots, d_1)(d_1 + 1, \dots, d_1 + d_2) \dots (n - d_k + 1, n - d_k + 2, \dots, n - 1, n) = \\ &= \begin{pmatrix} 1 & 2 & \dots & d_1 & d_1 + 1 & \dots & d_1 + d_2 & \dots & \dots & n - d_k + 1 & \dots & n \\ 2 & 3 & \dots & 1 & d_1 + 2 & \dots & d_1 + 1 & \dots & \dots & n - d_k + 2 & \dots & n - d_k + 1 \end{pmatrix} \end{aligned}$$

- 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:

$$\begin{aligned}
 & \sigma \cdot \tau_{d_1-1, d_1} \cdot \tau_{d_1-2, d_1-1} \cdot \dots \cdot \tau_{2,3} \cdot \tau_{1,2} = \\
 & = (1)(2) \dots (d_1-1)(d_1)(d_1+1, \dots, d_1+d_2) \dots (n-d_k+1, n-d_k+2, \dots, n-1, n) = \\
 & = \left(\begin{array}{cccccccccccc} 1 & 2 & \dots & d_1 & d_1+1 & \dots & d_1+d_2 & \dots & \dots & n-(d_k+1) & \dots & n \\ 1 & 2 & \dots & d_1 & d_1+2 & \dots & d_1+1 & \dots & \dots & n-(d_k+1)+1 & \dots & n-(d_k+1) \end{array} \right)
 \end{aligned}$$

- 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:

$$\text{sgn}(\sigma) = \text{sgn}(\sigma') = (-1)^{n-k}$$

□

6

Morfismi

Definizione 46: 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:

$$f(a + b) = f(a) + f(b), \forall a, b \in A$$

$$f(ab) = f(a)f(b), \forall a, b \in A$$

Osservazione 30

Dati due gruppi G ed H e un morfismo $f : G \rightarrow H$, si ha che:

1. $f(1_G) = 1_H$
2. $f(g^{-1}) = f(g)^{-1}, \forall g \in G$
3. $f(g^k) = f(g)^k, \forall g \in G, \forall k \in \mathbb{Z}$

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:

$$\begin{aligned} f(1_G) &= 1_H \implies f(g \cdot g^{-1}) = 1_H \implies f(g)f(g^{-1}) = 1_H \implies \\ &\implies f(g^{-1}) = 1_H \cdot f(g)^{-1} \implies f(g^{-1}) = f(g)^{-1} \end{aligned}$$

3. Dato $g \in G$ e dato $n \in \mathbb{N}$, per le proprietà del morfismo f ne segue che:

$$f(g^n) = f(\underbrace{g \cdot g \cdot \dots \cdot g}_{n \text{ volte}}) = \underbrace{f(g)f(g) \dots f(g)}_{n \text{ volte}} = f(g)^n$$

A questo punto, dato $k := -n \in \mathbb{Z}$, tramite il punto 2) e il punto appena dimostrato ne segue automaticamente che:

$$f(g^k) = f(g^{-n}) = f((g^n)^{-1}) = f(g^n)^{-1} = (f(g)^n)^{-1} = f(g)^{-n} = f(g)^k$$

□

Osservazione 31

Sia $f : G \rightarrow H$ un morfismo tra gruppi. Dato $g \in G \mid o(g) < +\infty$, si ha che

$$o(f(g)) \mid o(g)$$

Dimostrazione:

- Dalle proprietà dei morfismi, ne segue automaticamente che:

$$f(g)^{o(g)} = f(g^{o(g)}) = f(1_G) = 1_H \implies o(f(g)) \mid o(g)$$

□

6.1 Isomorfismi, Endomorfismi ed Automorfismi

Definizione 47: 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**

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 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, f risulta essere un isomorfismo tra \mathbb{Z}_n e H^n

2. • Sia G un gruppo e sia $g \in G$. La funzione $f : (\mathbb{Z}, +) \rightarrow (G, \cdot) : n \rightarrow g^n$ 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 4.11, 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

3. Dato il gruppo (G, \cdot) e $g \in G$, la funzione $f_g : G \rightarrow G : h \mapsto ghg^{-1}$ è un endomorfismo:

$$f_g(h)f_g(h') = (ghg^{-1})(gh'h^{-1}) = gh'hg^{-1} = f_g(hh')$$

Osservazione 32

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:

$$\pi(x+y) = [x+y] = [x] + [y] = \pi(x) + \pi(y)$$

$$\pi(xy) = [xy] = [x][y] = \pi(x)\pi(y)$$

□

Osservazione 33

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:

$$\begin{aligned} gh &= f(f^{-1}(g))f(f^{-1}(h)) \implies gh = f((f^{-1}(g)(f^{-1}(h))) \implies \\ \implies f^{-1}(gh) &= f^{-1}(f((f^{-1}(g)(f^{-1}(h)))) \implies f^{-1}(gh) = f^{-1}(g)f^{-1}(h) \end{aligned}$$

□

Osservazione 34

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:

$$h(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = h(x)h(y)$$

□

Definizione 48: 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:

$$G \cong H, H \cong K \implies \exists f : G \rightarrow H \text{ isomorfismo}, \exists g : H \rightarrow K \text{ isomorfismo} \implies$$

$$\implies g \circ f : G \rightarrow K \text{ isomorfismo} \implies G \cong K$$

□

Lemma 12

Sia $f : G \rightarrow G'$ un isomorfismo tra gruppi (dunque $G \cong G'$). Dato $g \in G \mid o(g) < +\infty$, si ha che:

$$o(g) = o(f(g))$$

Dimostrazione:

- Poiché f è un morfismo, per dimostrazione precedente ne segue che $o(f(g)) \mid o(g)$
- Inoltre, poiché f è un isomorfismo, sappiamo che esiste sempre l'isomorfismo inverso $f^{-1} : G' \rightarrow G$.

- A questo punto, ne segue che:

$$g^{o(f(g))} = f^{-1}(f(g^{o(f(g))})) = f^{-1}(f(g)^{o(f(g))}) = f^{-1}(1_H) = 1_G \implies o(g) \mid o(f(g))$$

- A questo punto, per anti-simmetria si ha che:

$$o(f(g)) \mid o(g), o(g) \mid o(f(g)) \implies o(g) = o(f(g))$$

□

Teorema 11: Isomorfismo tra sottogruppi ciclici

Sia $f : G \rightarrow G'$ un isomorfismo tra gruppi (dunque $G \cong G'$). Dato $g \in G \mid o(g) < +\infty$, si ha che:

$$H(g) \cong H(f(g))$$

Dimostrazione:

- Sia $h : H(g) \rightarrow H(f(g)) : x \mapsto f(x)$

- Notiamo che:

$$h(xx') = f(xx') = f(x)f(x') = h(x)h(x')$$

dunque h risulta essere un morfismo

- Essendo f un isomorfismo (dunque iniettivo), ne segue che:

$$\forall x, y \in H(f(g)) \quad h(x) = h(y) \implies f(x) = f(y) \implies x = y$$

dunque h risulta essere iniettiva

- Per il lemma precedente, si ha che

$$G \cong G' \implies o(g) = o(f(g)) \implies |H(g)| = |H(f(g))|$$

- Di conseguenza, poiché h è un morfismo iniettivo e poiché $|H(g)| = |H(f(g))|$, ne segue automaticamente che h sia un isomorfismo e dunque che $H(g) \cong H(f(g))$

□

6.2 Nucleo ed Immagine di un morfismo

Definizione 49: Nucleo ed Immagine di un morfismo

Dato un morfismo $f : G \rightarrow H$ definiamo $\ker(f)$ come **nucleo di f** e $\text{im}(f)$ come **immagine di f** , dove:

$$\ker(f) := \{g \in G \mid f(g) = 1_H\}$$

$$\text{im}(f) := \{y \in H \mid f(x) = y, \exists x \in G\}$$

Inoltre, si ha che $\ker(f) \leq G$ e $\text{im}(f) \leq H$

Dimostrazione:

- $\ker(f) \leq G$:
 - $f(1_G) = 1_H \implies 1_G \in \ker(f)$
 - $x, y \in \ker(f) \implies f(x) = f(y) = 1_H \implies f(xy) = f(x)f(y) = 1_H \cdot 1_H = 1_H \implies xy \in \ker(f)$
 - $x \in \ker(f) \implies f(x) = 1_H \implies 1_H = 1_H^{-1} = f(x)^{-1} = f(x^{-1}) \implies x^{-1} \in \ker(f)$
- $\text{im}(f) \leq H$:
 - $f(1_G) = 1_H \implies 1_H \in \text{im}(f)$
 - $x, y \in \text{im}(f) \implies x = f(g), y = f(h) \implies xy = f(g)f(h) = f(gh) \implies xy \in \text{im}(f)$
 - $x \in \text{im}(f) \implies x = f(g) \implies x^{-1} = f(g)^{-1} = f(g^{-1}) \implies x^{-1} \in \text{im}(f)$

□

Osservazione 35

Un morfismo è **iniettivo** se e solo se il nucleo è **semplice**, ossia $\ker(f) = \{1_G\}$

Dimostrazione:

- Poiché $\ker(f) \leq G \implies 1_G \in \ker(f)$, supponiamo per assurdo che f iniettiva e che $\exists x \neq 1_G \in \ker(f)$:

$$g \neq 1_G \in \ker(f) \implies f(g) = 1_H = f(1_G)$$

contraddicendo l'ipotesi per cui f sia iniettiva, dunque l'unica possibilità è che

$$\nexists g \neq 1_G \in \ker(f) \implies \ker(f) = \{1_G\}$$

- Supponiamo invece che $\ker(f) = \{1_G\}$. 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 $\ker(f) = \{1_G\}$, 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

□

Osservazione 36

Se $f : A \rightarrow B$ è un morfismo di anelli, allora:

$$\ker(f) := \{a \in A \mid f(a) = 0_B\}$$

$$\operatorname{im}(f) := \{b \in B \mid f(a) = b, \exists a \in A\}$$

6.3 Primo teorema d'isomorfismo

Definizione 50: Sottoanello

Sia A un anello. Definiamo $(B, +, \cdot) \leq (A, +, \cdot)$ come **sottoanello** se:

- $(B, +) \leq (A, +)$
- $x, y \in B \implies xy \in B$

Osservazione 37

Se $f : A \rightarrow B$ è un morfismo di anelli, allora

- $\ker(f) \triangleleft A$
- $\operatorname{im}(f) \leq B$ sottoanello

Dimostrazione:

- Abbiamo già dimostrato che $\ker(f) \leq G$ e $\operatorname{im}(f) \leq B$.
- $x \in \ker(f), y \in A \implies f(xy) = f(x)f(y) = 0_B \cdot f(y) = 0_B \implies xy \in \ker(f)$

- $x, y \in \text{im}(f) \iff x = f(a), y = f(b), \exists a, b \in A \implies xy = f(a)f(b) = f(ab) \implies xy \in \text{im}(f)$

□

Teorema 12: Primo teorema d'isomorfismo

Se $f : A \rightarrow B$ è un morfismo tra anelli, allora

$$A/\ker(f) \cong \text{im}(f)$$

Dimostrazione:

- Mostriamo che esiste $\varphi : A/\ker(f) \rightarrow \text{im}(f) : [a] \mapsto f(a)$ 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 $\text{im}(f)$, coincide con la sua immagine, ossia $\text{im}(\varphi)$:

$$\begin{aligned} y \in \text{im}(\varphi) &\iff \exists [a] \in A/\ker(f) \mid \varphi([a]) = y \iff \\ &\iff \exists a \in A \mid f(a) = y \iff y \in \text{im}(f) \end{aligned}$$

- Concludiamo quindi che $\varphi : A/\ker(f) \rightarrow \text{im}(f)$ è un **isomorfismo** e dunque che

$$A/\ker(f) \cong \text{im}(f)$$

□

6.4 Sottogruppi normali

Definizione 51: 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*)

Definizione 52: 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

Osservazione 38

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*)

Osservazione 39

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:

$$|G/H_{sx}| = \frac{|G|}{|H|} = |G/H_{dx}|$$

□

Osservazione 40

La **classe neutra**, ossia generata dall'elemento neutro di G , è sia una classe laterale **sinistra** sia una classe laterale **destra**:

$$[1_G]_{sx} = 1_G \cdot H = H = H \cdot 1_G = [1_G]_{dx}$$

Definizione 53: 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 $gh = hg, \forall g \in G, \forall h \in H$)

Proposizione 35

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:

$$gh \in gH \implies g \in G, h \in H \implies x := ghg^{-1} \in H \implies$$

$$\implies xg = ghg^{-1}g \in Hg \implies xg = gh \implies gh \in Hg \implies gH \subseteq Hg$$

– 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 $H \trianglelefteq G$

□

Osservazione 41

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 $H \trianglelefteq G$

□

Proposizione 36

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
 - $([x][y])[z] = [xy][z] = [xyz] = [x][yz] = [x]([y][z])$
 - $\forall [x] \in G/H, \exists [1_G] \in G/H \mid [x][1_G] = [x \cdot 1_G] = [x]$
 - $\forall [x] \in G/H, \exists [x]^{-1} \in G/H \mid [x][x]^{-1} = [x][x^{-1}] = [xx^{-1}][1_G]$

□

Corollario 19

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:

$$[x], [y] \in G/H \implies [x][y] = [xy] = [yx] = [y][x]$$

□

Osservazione 42

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:

$$G/H_{sx} = \{H, G - H\}$$

$$G/H_{dx} = \{H, G - H\}$$

□

Corollario 20

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 $\mathcal{A}_n \trianglelefteq \mathcal{S}_n$

□

Osservazione 43

Se $f : G \rightarrow H$ è un morfismo di gruppi, allora $\ker(f) \trianglelefteq G$ e $\operatorname{im}(f) \leq H$

Dimostrazione:

- Sappiamo già che $\ker(f) \leq G$ e $\operatorname{im}(f) \leq H$
- Verifichiamo quindi che $\ker(f) \trianglelefteq G$

$$\begin{aligned} g \in G, h \in \ker(f) &\implies f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g) \cdot 1_H \cdot f(g)^{-1} = \\ &= f(g)f(g)^{-1} = 1_H \implies ghg^{-1} \in \ker(f) \implies \ker(f) \trianglelefteq G \end{aligned}$$

□

Teorema 13: Primo teorema d'isomorfismo

Se $f : G \rightarrow H$ è un morfismo tra gruppi, allora:

$$G/\ker(f) \cong \operatorname{im}(f)$$

Teorema fondamentale di

Dimostrazione:

- Poiché $\ker(f) \trianglelefteq G$, sappiamo che $(G/\ker(f), \cdot)$ 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)

□

Proposizione 37

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 primo teorema d'isomorfismo si ha che:

$$\mathbb{Z}/\ker(f) \cong \text{im}(f)$$

- Tuttavia, notiamo che:

$$\text{im}(f) = \{f(n) \mid n \in \mathbb{Z}\} = \{g^n \mid n \in \mathbb{Z}\} = H(g)$$

$$\ker(f) = \{n \in \mathbb{Z} \mid g^n = 1_G\} = I(g)$$

- Dunque, si ha che:

$$\mathbb{Z}/I(g) = \mathbb{Z}/\ker(f) \cong \text{im}(f) = H(g)$$

- 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:

$$\mathbb{Z}_d := \mathbb{Z}/I(d) = \mathbb{Z}/I(g) = \mathbb{Z}/\ker(f) \cong \text{im}(f) = H(g)$$

- 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:

$$H(g) = \text{im}(f) \cong \mathbb{Z}/\ker(f) = \mathbb{Z}/I(g) = \mathbb{Z}/I(d) = \begin{cases} \mathbb{Z}_0 \cong \mathbb{Z} & \text{se } d = 0 \\ \mathbb{Z}_d & \text{se } d > 0 \end{cases}$$

□

Corollario 21

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:

$$G = H(g) \cong \mathbb{Z}_n$$

□

Corollario 22

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:

$$o(g) = p \implies G = H(g) \cong \mathbb{Z}_p$$

□

Osservazione 44

Sia G un gruppo. Se $H \leq G$ allora la proiezione canonica al quoziente $\pi : (G, \cdot) \rightarrow (G/H, \cdot) : x \rightarrow [x]$ è un morfismo suriettivo e $\ker(\pi) = H$

Dimostrazione:

- Sappiamo già che $\pi : (G, \cdot) \rightarrow (G/H, \cdot) : x \rightarrow [x]$ sia un morfismo suriettivo

- Verifichiamo quindi che $\ker(f) = H$:

$$g \in \ker(\pi) \iff \pi(g) = [1_G] \iff [g] = [1_G] = H \iff g \in [g] = H$$

□

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 primo teorema d'isomorfismo, si ha che:

$$\mathcal{S}_n / \ker(\text{sgn}) \cong \text{im}(\text{sgn})$$

- Inoltre, si ha che:

$$\begin{aligned} \ker(\text{sgn}) &= \{\sigma \in \mathcal{S}_n \mid \text{sgn}(\sigma) = +1\} = \mathcal{A}_n \trianglelefteq \mathcal{S}_n \implies \\ \implies [\mathcal{S}_n : \ker(\text{sgn})] &= [\mathcal{S}_n : \mathcal{A}_n] = 2 \implies |\text{im}(\text{sgn})| = 2 \implies \text{im}(\text{sgn}) = \{+1, -1\} \end{aligned}$$

6.5 Gruppi diedrali

Definizione 54: 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 $\rho\sigma(i) = \rho(\sigma(i))$

Osservazione 45

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:

$$\sigma_n = \sigma_0 \implies \sigma_{n+k} = \sigma_k$$

Osservazione 46

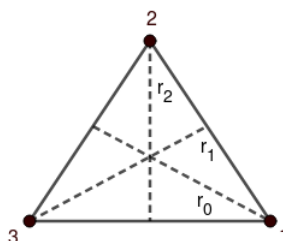
Per definizione stessa, ogni riflessione a specchio è uguale alla sua inversa.

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:

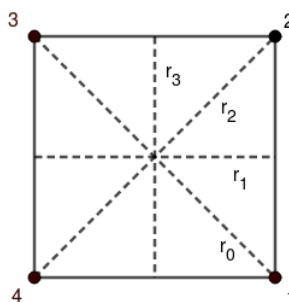
- Consideriamo il gruppo \mathcal{D}_3 , corrispondente alle simmetrie di un triangolo equilatero.



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.

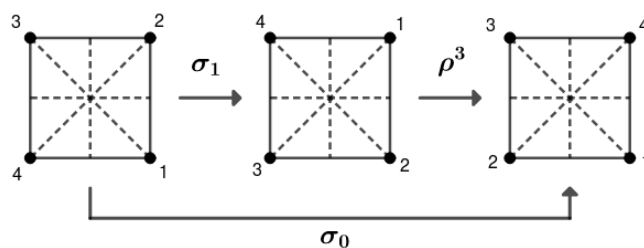


In tal caso, abbiamo che:

$$\mathcal{D}_4 := \{1, \rho, \rho^2, \rho^3, \sigma_0, \sigma_1, \sigma_2, \sigma_3\}$$

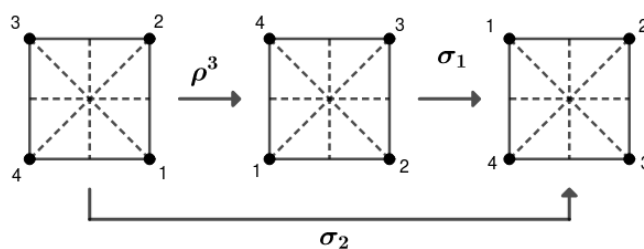
Notiamo inoltre come in \mathcal{D}_4 si ha:

$$\rho^3 \sigma_1 = \sigma_0$$



E che:

$$\sigma_1 \rho^3 = \sigma_2$$



Dunque, concludiamo che il prodotto non sia commutativo:

$$\rho^3 \sigma_1 \neq \sigma_1 \rho^3$$

Osservazione 47

Dato il gruppo \mathcal{D}_n , si ha che:

- $\rho^i \rho^j = \rho^{i+j(\bmod n)}$
- $\sigma_i \sigma_j = \rho^{i-j(\bmod n)}$
- $\rho^i \sigma_j = \sigma_{i+j(\bmod n)}$
- $\sigma_i \rho^j = \sigma_{i-j(\bmod n)}$

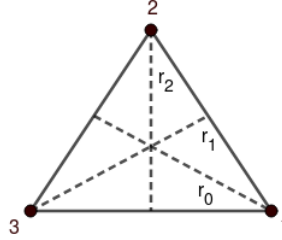
Proposizione 38

Numerando i vertici del poligono, ogni simmetria **corrisponde** ad una permutazione dei vertici, dunque si verifica che \mathcal{D}_n è **isomorfo** ad un sottogruppo **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:

$$\begin{aligned} 1 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & \rho &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & \rho^2 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\ \sigma_0 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} & \sigma_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} & \sigma_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \end{aligned}$$

Corollario 23

Dato il gruppo \mathcal{D}_n e dato $H_n \subseteq \mathcal{S}_n$ dove:

$$H_n := \{\sigma_\alpha \in \mathcal{S}_n \mid \sigma_\alpha = \alpha, \exists \alpha \in \mathcal{D}_n\}$$

si ha che:

$$\mathcal{D}_n \cong H_n \leq \mathcal{S}_n$$

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

Definizione 55: Gruppo di Klein

Definiamo come **gruppo di Klein** (o gruppo quadrimio) 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 $\mathcal{D}_2 \cong \mathcal{K}_4$

Proposizione 39

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 $\nexists a \in G \mid o(a) = 4$, 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:

$$G \cong \mathcal{K}_4$$

□

Teorema 14: 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

$$\exists g \in G \mid o(g) = q \implies |G| = o(g) \implies G = H(g)$$

Proposizione 40

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:

$$o(\beta) = 2 \quad o(\alpha^{i-j}) = \begin{cases} o(1) = 1 & \text{se } i = j \\ o(\alpha^k) = 3 & \text{se } i \neq j \end{cases}$$

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 $|\mathcal{S}_n| = n! = 6$.

- Affinché l'isomorfismo esista si ha necessariamente che $|H| = |\mathcal{D}_3| = 6$, implicando quindi che

$$H_3 \leq \mathcal{S}_3, |H_3| = |\mathcal{S}_3| \implies G \cong \mathcal{D}_3 \cong H = \mathcal{S}_3$$

□

Esempio:

1. • Vogliamo stabilire se \mathbb{Z}_9^* e \mathbb{Z}_{14}^* siano isomorfi tra loro.
- Prima di tutto, calcoliamo \mathbb{Z}_9^* e \mathbb{Z}_{14}^* :

$$\mathbb{Z}_9^* = \{[1], [2], [4], [5], [7], [8]\}$$

$$\mathbb{Z}_{14}^* = \{[1], [3], [5], [9], [11], [13]\}$$

- Notiamo quindi che $|\mathbb{Z}_9^*| = |\mathbb{Z}_{14}^*| = 6$, implicando che essi siano potenzialmente isomorfi tra loro.
- A questo punto, calcoliamo gli ordini degli elementi:

\mathbb{Z}_9^*		\mathbb{Z}_{14}^*	
Elemento	Ordine	Elemento	Ordine
[1]	1	[1]	1
[2]	6	[3]	6
[4]	3	[5]	6
[5]	6	[9]	3
[7]	3	[11]	3
[8]	2	[13]	2

- Poiché entrambi i gruppi possiedono un elemento di ordine 6, per la proposizione precedente si ha che

$$\mathbb{Z}_9^* \cong \mathbb{Z}_6 \wedge \mathbb{Z}_{14}^* \cong \mathbb{Z}_6 \implies \mathbb{Z}_9^* \cong \mathbb{Z}_6 \cong \mathbb{Z}_{14}^*$$

dunque i due gruppi sono isomorfi tra loro

- Vogliamo stabilire se \mathbb{Z}_{24}^* e \mathbb{Z}_{30}^* siano isomorfi tra loro.
- Prima di tutto, calcoliamo \mathbb{Z}_{24}^* e \mathbb{Z}_{30}^* :

$$\mathbb{Z}_{24}^* = \{[1], [5], [7], [11], [13], [17], [19], [23]\}$$

$$\mathbb{Z}_{30}^* = \{[1], [7], [11], [13], [17], [19], [23], [29]\}$$

- Notiamo quindi che $|\mathbb{Z}_{24}^*| = |\mathbb{Z}_{30}^*| = 8$, implicando che essi siano potenzialmente isomorfi tra loro.
- A questo punto, calcoliamo gli ordini degli elementi:

\mathbb{Z}_{24}^*		\mathbb{Z}_{30}^*	
Elemento	Ordine	Elemento	Ordine
[1]	1	[1]	1
[5]	2	[7]	4
[7]	2	[11]	2
[11]	2	[13]	4
[13]	2	[17]	4
[17]	2	[19]	2
[19]	2	[23]	4
[24]	2	[29]	2

- Poiché gli ordini degli elementi sono diversi tra loro, per il teorema di isomorfismo tra sottogruppi ciclici (sezione 6.1) risulta impossibile che \mathbb{Z}_{24}^* e \mathbb{Z}_{30}^* siano isomorfi tra loro

7

Polinomi

Definizione 56: 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.

□

Osservazione 48

Se K è un campo, allora $K[x]$ è un anello commutativo, poiché non ammette comunque l'esistenza dell'inverso nel prodotto

Definizione 57: 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)
- $p(x) = a_0 + a_1x + \dots + a_nx^n \neq 0, a_n \neq 0 \implies \deg(p(x)) = n$

Definizione 58: 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

Proposizione 41

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

Osservazione 49

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

$$p(x) \cdot q(x) = \sum_{i=0}^n \left(\sum_{j=0}^m a_i b_j x^{i+j} \right) = a_0 b_0 + a_0 b_1 x^1 + \dots + a_n b_m x^{n+m}$$

$$\text{allora } \deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x)) = n + m$$

□

Proposizione 42

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

Teorema 15: 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:

$$\begin{aligned} b(x)q_1(x) + r_1(x) &= b(x)q_2(x) + r_2(x) \implies b(x)[q_1(x) - q_2(x)] = r_2(x) - r_1(x) \implies \\ &\implies \deg(r_2(x) - r_1(x)) = \deg(b(x)) + \deg(q_1(x) - q_2(x)) \end{aligned}$$

- Nel caso in cui $\deg(q_1(x) - q_2(x)) \geq 0$, avremmo $\deg(r_2(x) - r_1(x)) \geq \deg(b(x))$, contraddicendo l'ipotesi. Di conseguenza, l'unica possibilità è

$$\deg(q_1(x) - q_2(x)) = -\infty \iff q_1(x) - q_2(x) = 0 \iff q_1(x) = q_2(x)$$

- A questo punto, quindi, si ha che:

$$\begin{aligned} b(x)[q_1(x) - q_2(x)] &= r_2(x) - r_1(x) \implies b(x) \cdot 0 = r_1(x) - r_1(x) \iff \\ &\iff 0 = r_2(x) - r_1(x) \iff r_1(x) = r_2(x) \end{aligned}$$

□

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:

$$2x^4 + 3x^3 - 2x^2 + x - 4 = (x^2 - x + 1)(2x^2 + 5x + 1) + 3x - 5$$

Metodo 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:

	a_n	a_{n-1}	\dots	a_1	a_0
c		cq_{n-1}	\dots	cq_1	cq_0
	q_{n-1}	q_{n-2}	\dots	q_0	r_0

Esempio:

- Calcolare la divisione tra $a(x) = x^4 - 3x^3 + 2x - 5$ e $b(x) = x + 2$

	1	-3	0	2	-5
-2		-2	10	-20	36
	1	-5	10	-18	31

Dunque si ha che:

$$x^4 - 3x^3 + 2x - 5 = (x + 2)(x^3 - 5x^2 + 10x - 18) + 31$$

Teorema 16: 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:

$$\bullet \quad x - c \mid p(x) \implies p(c) = 0$$

$$x - c \mid p(x) \implies p(x) = (x - c)q(x) \implies p(c) = (c - c)q(c) = 0$$

$$\bullet \quad p(c) = 0 \implies x - c \mid p(x)$$

– Siano $q(x)$ e $r(x)$ il quoziente e il resto della divisione di $p(x)$ per $(x - c)$

$$p(x) = (x - c)q(x) + r(x)$$

– Poiché per definizione stessa di divisione con resto tra polinomi si ha che $\deg(r(x)) < \deg(x - c)$, ne segue che:

$$\deg(r(x)) < \deg(x - c) \implies \deg(r(x)) < 1 \implies r := r(x) \in K$$

– Infine, per ipotesi si ha che

$$\begin{aligned} 0 = p(c) &= (c - c)q(c) + r \implies 0 = (c - c)q(c) + r \implies \\ &\implies 0 = 0 + r \implies r = 0 \end{aligned}$$

dunque, la divisione non ha resto, implicando che:

$$(x - c) \mid p(x)$$

□

Proposizione 43

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

Proposizione 44

L'anello commutativo $K[x]$ è un **dominio di integrità** poiché vale la **legge di annullamento del prodotto**

Corollario 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*)

Teorema 17

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 $p(x)$

□

Definizione 59: MCD di polinomi

Dati $a_1(x), \dots, a_n(x) \in K[x]$, definiamo $d(x) \in K[x]$ come **massimo comun divisore** di $a_1(x), \dots, a_n(x)$, indicato come $d(x) := \text{MCD}(a_1(x), \dots, a_n(x))$, se dato $k(x) \in K[x]$ si verifica che

$$k(x) \mid a_1(x) \wedge \dots \wedge k(x) \mid a_n(x) \iff k(x) \mid d(x)$$

Proposizione 45: Identità di Bézout tra polinomi

Dati $a_1(x), \dots, a_n(x) \in K[x]$ e dato $d(x) := \text{MCD}(a_1(x), \dots, a_n(x))$, si ha che:

$$I(a_1(x), \dots, a_n(x)) = I(d(x))$$

In altre parole, si ha che:

$$\exists x_1(x), \dots, x_n(x) \in \mathbb{Z} \mid a_1(x)x_1(x) + \dots + a_n(x)x_n(x) = d(x)$$

che definiamo come **identità di Bézout** tra polinomi.

Definizione 60: mcm di polinomi

Dati $a_1(x), \dots, a_n(x) \in K[x]$, definiamo $m(x) \in K[x]$ come **minimo comune multiplo** di $a_1(x), \dots, a_n(x)$, indicato come $m(x) := \text{mcm}(a_1(x), \dots, a_n(x))$, se dato $k(x) \in K[x]$ si verifica che

$$a_1(x) \mid k(x) \wedge \dots \wedge a_n(x) \mid k(x) \iff m(x) \mid k(x)$$

Osservazione 50

Poiché $K[x]$ è un 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** $a_n = 1$

Definizione 61: 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 $a_n = 1$

Proposizione 46: Prodotto tra mcm e MCD di polinomi

Dati $a(x), b(x) \in K[x]$, si ha che:

$$\text{mcm}(a(x), b(x)) \cdot \text{MCD}(a(x), b(x)) = a(x)b(x)$$

(*dimostrazione omessa*)

Teorema 18: Radici comuni tra due polinomi

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:

$$d(c) = 0 \implies (x - c) \mid d(x), d(x) \mid a_i(x), \forall i \in [1, n] \implies (x - c) \mid a_i(x), \forall i \in [1, n]$$

□

Proposizione 47

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 $p(x) \mid a(x)b(x)$:

$$p(x) \mid a(x)b(x) \iff a(x)b(x) = p(x)k(x), \exists k(x) \in K[x]$$

- Se $p(x) \nmid a(x)$, si ha che $d(x) := \text{MCD}(p(x), a(x)) = 1$. Dunque, tramite l'identità di Bézout 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 $d(x) := \text{MCD}(p(x), b(x)) = 1$. Dunque, seguendo gli stessi passaggi otteniamo che $p(x) \mid a(x)$
- Concludiamo quindi che se $p(x)$ è irriducibile, allora:

$$p(x) \mid a(x)b(x) \implies p(x) \mid a(x) \vee p(x) \mid b(x)$$

□

Lemma 13

Dato $p(x) \in K[x]$, si ha che:

$$\deg(p(x)) = 1 \implies p(x) \text{ irriducibile}$$

Dimostrazione:

- Se $\deg(p(x)) = 1$ allora

$$p(x) = a(x)b(x) \implies \begin{cases} \deg(a(x)) = 0, \deg(b(x)) = 1 \implies a(x) \in \mathbb{C}[x]^* \\ \deg(a(x)) = 1, \deg(b(x)) = 0 \implies b(x) \in \mathbb{C}[x]^* \end{cases}$$

dunque $p(x)$ è irriducibile

□

Proposizione 48

Dato $p(x) \in \mathbb{C}[x]$, si ha che:

$$p(x) \in \mathbb{C}[x] \text{ irriducibile} \iff \deg(p(x)) = 1$$

Dimostrazione:

- Sappiamo già che $\deg(p(x)) = 1 \implies p(x)$ irriducibile
- Consideriamo quindi il caso in cui $\deg(p(x)) = 0$, allora

$$\deg(p(x)) = 0 \iff p(x) \in \mathbb{C}^*$$

dunque $p(x)$ non può essere irriducibile per definizione stessa

- Sia invece $\deg(p(x)) > 1$. 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 $q(x) \notin \mathbb{C}[x]^*$.

- Dunque si ha che

$$\deg(p(x)) \neq 1 \implies p(x) \text{ non irriducibile}$$

che per contronominale implica che

$$p(x) \text{ irriducibile} \implies \deg(p(x)) = 1$$

□

Proposizione 49

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 $\deg(p(x)) = 2 \implies p(x) = ax^2 + bx + c, \Delta := b^2 - 4ac$

Dimostrazione:

- Poiché $\mathbb{R}[x] \subset \mathbb{C}[x]$, la dimostrazione in entrambi i lati dei casi con $\deg(p(x)) = 1$ è analoga alla precedente
- Supponiamo quindi per assurdo che $\deg(p(x)) = 2, \Delta < 0$ e che $p(x)$ non sia irriducibile, implicando che:

$$\exists a(x)b(x) \in \mathbb{R}[x] - \mathbb{R}[x]^* \mid p(x) = a(x)b(x) \wedge \deg(p(x)) = 2$$

$$\implies \deg(a(x)) = \deg(b(x)) = 1 \implies$$

$$\implies \begin{cases} \exists c, d \in \mathbb{R} \mid a(x) = cx + d \implies a(-c^{-1}d) = 0 \iff (x + c^{-1}d) \mid a(x) \\ \exists f, g \in \mathbb{R} \mid b(x) = fx + g \implies b(-f^{-1}g) = 0 \iff (x + f^{-1}g) \mid b(x) \end{cases} \implies$$

$$\implies \begin{cases} (x + c^{-1}d) \mid a(x), a(x) \mid p(x) \implies (x + c^{-1}d) \mid p(x) \iff p(-c^{-1}d) = 0 \\ (x + f^{-1}g) \mid b(x), b(x) \mid p(x) \implies (x + f^{-1}g) \mid p(x) \iff p(-f^{-1}g) = 0 \end{cases}$$

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:

$$\deg(p(x)) = 2, \Delta < 0 \implies p(x) \in \mathbb{R}[x] \text{ irriducibile}$$

- Sia quindi $p(x) := a_0 + \dots + a_n x^n \in \mathbb{R}[x] \subset \mathbb{C}[x]$ irriducibile con $\deg(p(x)) > 1$. Per il teorema fondamentale dell'algebra, $\exists z := c + id \in \mathbb{C} \mid p(z) = 0 \iff (x - z) \mid p(x)$
- Poiché $a_1, \dots, a_n \in \mathbb{R}$, si ha che:

$$\forall j \in [1, n], \exists d_j \in \mathbb{R} \mid a_j := d_j + i \cdot 0 = d_j - i \cdot 0 =: \overline{a_j} \implies a_j = \overline{a_j}, \forall j \in [1, n]$$

dunque, per le proprietà dei complessi coniugati (sezione 2.1), ne segue che:

$$p(\overline{z}) = a_0 + \dots a_n \overline{z}^n = a_0 + \dots a_n \overline{z}^n = \overline{a_0} + \dots \overline{a_n} \overline{z}^n = \overline{a_0} + \dots \overline{a_n} \overline{z}^n =$$

$$\overline{a_0 + \dots + a_n z^n} = \overline{p(z)} = \overline{0} = 0 \implies p(\overline{z}) = 0 \iff (x - \overline{z}) \mid p(x)$$

dove per definizione si ha $\overline{z} = c - id$

- Nel caso in cui $d = 0$, ne seguirebbe che $z = \overline{z}$, implicando che:

$$(x - z) \mid p \iff p(x) = q(x)(x - z), \exists q(x) \in \mathbb{R}[x] \implies$$

$$\implies \deg(q(x)) + \deg(x - z) = \deg(p(x)) > 1 \implies$$

$$\implies \deg(q(x)) + 1 > 1 \implies \deg(q(x)) > 0 \implies q(x) \notin K^*$$

rendendo quindi tale caso è impossibile, poiché altrimenti si avrebbe che $p(x)$ non sia irriducibile in quanto $q(x), (x - z) \notin K^*$

- Sia quindi $d \neq 0$, implicando che $z \neq \bar{z}$:

$$\begin{aligned} (x - z) \mid p(x), (x - \bar{z}) \mid p(x) &\implies (x - z)(x - \bar{z}) \mid p(x) \implies \\ &\implies x^2 - \bar{z}x - zx + z \cdot \bar{z} \mid p(x) \implies x^2 - (\bar{z} + z)x + z \cdot \bar{z} \mid p(x) \implies \\ &\implies x^2 - (c - id + c + id)x + (c + id)(c - id) \mid p(x) \implies x^2 - 2cx + c^2 + d^2 \mid p(x) \end{aligned}$$

- Poiché $p(x)$ è irriducibile, l'unica possibilità è:

$$\begin{aligned} x^2 - 2cx + c^2 + d^2 \mid p(x) &\implies p(x) = k(x^2 - 2cx + c^2 + d^2), \exists k \in \mathbb{R}[x]^* = \mathbb{R}^* \implies \\ &\implies p(x) = kx^2 - 2kcx + kc^2 + kd^2 \implies \Delta = (-2kc)^2 - 4k^2(c^2 + d^2) \implies \\ &\implies \Delta = 4k^2c^2 - 4k^2c^2 - 4k^2d^2 \implies \Delta = -4k^2d^2 < 0 \end{aligned}$$

□

Teorema 19: Fattorizzazione in polinomi irriducibili e monici

Dato $p(x) \neq 0 \in K[x]$, si ha che:

$$\exists! q_1(x), \dots, q_k(x) \neq 0 \in K[x], \exists c \in K^* \mid p(x) = c \cdot q_1(x) \cdot \dots \cdot q_k(x)$$

dove $q_1(x), \dots, q_k(x)$ sono **polinomi monici e irriducibili**

Dimostrazione esistenza:

- Supponiamo che $\deg(p(x)) = 1$, implicando che $p(x) = ax + b, \exists a, b \neq 0 \in K$
- Poiché $a, b \neq 0 \implies a, b \in K^* \implies \exists a^{-1}, b^{-1} \in K^*$, ne segue che

$$p(x) = ax + b \implies p(x) = a \left(x + \frac{b}{a} \right) \implies p(x) = a(x + ba^{-1})$$

dove a e $\deg(x - ba^{-1}) = 1 \implies (x - ba^{-1})$ irriducibile, dunque esiste una fattorizzazione di $p(x)$ in polinomi monici ed irriducibili

- Sia quindi $p(x) \in K[x] \mid \deg(p(x)) > 1$ dove

$$\exists a(x), b(x) \in K[x] \mid p(x) = d(x)f(x)$$

e supponiamo per ipotesi induttiva che $a(x)$ e $b(x)$ siano fattorizzabili in polinomi monici ed irriducibili:

$$\exists! q_1(x), \dots, q_k(x) \in K[x], \exists c \in K^* \mid d(x) = c \cdot q_1(x) \cdot \dots \cdot q_k(x)$$

$$\exists! q'_1(x), \dots, q'_k(x) \in K[x], \exists c' \in K^* \mid f(x) = c' \cdot q'_1(x) \cdot \dots \cdot q'_k(x)$$

da cui ne segue che:

$$\begin{aligned} p(x) = d(x)f(x) &= c \cdot q_1(x) \cdot \dots \cdot q_k(x) \cdot c' \cdot q'_1(x) \cdot \dots \cdot q'_k(x) = \\ &= (c \cdot c') \cdot q_1(x) \cdot \dots \cdot q_k(x) \cdot q'_1(x) \cdot \dots \cdot q'_k(x) \end{aligned}$$

dunque $p(x)$ è fattorizzabile in polinomi monici ed irriducibili

Dimostrazione unicità:

- Se $\deg(p(x)) = 0$ allora $\exists! c \in K^* \mid p(x) = c$
- Sia quindi $\deg(p(x)) > 0$. Notiamo inoltre che dato $p(x) := a_0 + a_1x + \dots + a_nx^n$, affinché la fattorizzazione possa essere in polinomi monici ed irriducibili ne segue necessariamente che $c = c' = a_n$.
- Supponiamo quindi che esistano due fattorizzazioni possibili in polinomi monici ed irriducibili per $p(x)$:

$$c \cdot q_1(x) \cdot \dots \cdot q_k(x) = p(x) = c' \cdot q'_1(x) \cdot \dots \cdot q'_j(x) \implies$$

$$c \cdot q_1(x) \cdot \dots \cdot q_k(x) = c' \cdot q'_1(x) \cdot \dots \cdot q'_j(x) \implies q_1(x) \mid q'_1(x) \cdot \dots \cdot q'_j(x)$$

- Tuttavia, poiché $q_1(x)$ irriducibile se e solo se è primo, ne segue che:

$$q'_1(x) \cdot \dots \cdot q'_j(x) \mid q'_1(x) \vee \dots \vee q_1(x) \mid q'_j(x)$$

- Per comodità, assumiamo che $q'_1(x)$ il polinomio per cui $q_1(x) \mid q'_1(x)$:

$$q_1(x) \mid q'_1(x) \iff q'_1(x) = d \cdot q_1(x), \exists d \in K^* \implies$$

$$c \cdot q_1(x) \cdot \dots \cdot q_k(x) = c' \cdot d \cdot q_1(x) \cdot \dots \cdot q'_j(x) \implies$$

$$\implies c \cdot q_2(x) \cdot \dots \cdot q_k(x) = \frac{p(x)}{q_1(x)} = c' \cdot d \cdot q'_2(x) \cdot \dots \cdot q'_j(x)$$

- Poiché $\deg\left(\frac{p(x)}{q_1(x)}\right) < \deg(p(x))$ possiamo concludere che $k = k$ e, a meno di riordinare i fattori, possiamo assumere che $q_2(x) = q'_2(x), \dots, q_k(x) = q'_j(x)$

□

Teorema 20

Sia $p(x) := a_0 + \dots + a_nx^n \in \mathbb{Z}[x]$ dove $a_0, a_n \neq 0$. Se $\frac{a}{b} \in \mathbb{Q}$ è radice di $p(x)$ e $\text{MCD}(a, b) = 1$, allora

$$p\left(\frac{a}{b}\right) = 0 \implies a \mid a_0, b \mid a_n$$

e di conseguenza che:

$$a \nmid a_0 \vee b \nmid a_n \implies p\left(\frac{a}{b}\right) \neq 0$$

Dimostrazione:

- Supponendo che $\frac{a}{b} \in \mathbb{Q} \mid p\left(\frac{a}{b}\right) = 0, \text{MCD}(a, b) = 1$, ne segue che:

$$0 = p\left(\frac{a}{b}\right) = a_0 + a_1 \cdot \left(\frac{a}{b}\right) + \dots + a_n \cdot \left(\frac{a}{b}\right)^n \implies$$

$$\implies b^n \cdot 0 = b^n \left(a_0 + a_1 \cdot \left(\frac{a}{b}\right) + \dots + a_n \cdot \left(\frac{a}{b}\right)^n \right) \implies$$

$$\begin{aligned}
&\implies 0 = a_0 b^n + \dots + a_{n-1} \cdot a^{n-1} \cdot b + a_n a^n \implies \\
&\implies a_n a^n = -a_0 b^n - \dots - a_{n-1} \cdot a^{n-1} \cdot b \implies \\
&\implies a_n a^n \cdot \frac{1}{b} = -a_0 b^{n-1} - \dots - a_{n-1} \cdot a^{n-1} \implies b \mid a_n a^n
\end{aligned}$$

- Poiché $\text{MCD}(a, b) = 1 \implies \text{MCD}(a^n, b) = 1$, allora

$$b \mid a_n a^n \implies b \mid a_n$$

- Analogamente, seguendo gli stessi passaggi arriviamo a dimostrare che $\text{MCD}(a, b) = 1 \implies \text{MCD}(a, b^n) = 1$ 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

$$p\left(\frac{a}{b}\right) \implies a \mid 30, b \mid 1$$

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

$$p\left(\frac{a}{b}\right) \implies a \mid -1, b \mid 6$$

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

Lemma 14

Dato $p \in \mathbb{P}$, si ha che:

$$\prod_{0 < a < p} (x - a) \equiv x^{p-1} - 1 \pmod{p}$$

Dimostrazione:

- Sia $q(x) := x^{p-1} - [1] \in \mathbb{Z}_p$. Per il piccolo teorema di Fermat, dato $0 < a < p$ si ha che:

$$\begin{aligned} a^{p-1} &\equiv 1 \pmod{p} \implies a^{p-1} - 1 \equiv 0 \pmod{p} \implies \\ &\implies q([a]) \equiv 0 \pmod{p} \iff x - [a] \mid q(x) \end{aligned}$$

- Dunque, si ha che:

$$\begin{aligned} x - [a] \mid q(x), \forall 0 < a < p &\implies \prod_{0 < a < p} (x - [a]) \mid q(x) \implies \\ &\implies q(x) = k \cdot \prod_{0 < a < p} (x - [a]), \exists k \in \mathbb{Z} \implies \end{aligned}$$

ottenendo quindi una fattorizzazione in polinomi monici ed irriducibili

- Poiché il coefficiente direttore di $q(x)$ è 1, affinché la fattorizzazione sia valida ne segue necessariamente che $k = 1$, concludendo che:

$$\prod_{0 < a < p} (x - a) \equiv x^{p-1} - 1 \pmod{p}$$

□

Lemma 15

Dato $d \in \mathbb{N}$ tale che $d \mid p - 1$, l'equazione $x^d \equiv 1 \pmod{p}$ ammette d soluzioni distinte in \mathbb{Z}_p

Dimostrazione:

- Sia $d \in \mathbb{N}$ tale che $d \mid p - 1$. Ne segue che:

$$d \mid p - 1 \implies p - 1 = dk, \exists k \in \mathbb{Z}$$

- Per dimostrazione precedente, si ha che:

$$\begin{aligned} \prod_{0 < a < p} (x - a) &\equiv x^{p-1} - 1 \pmod{p} \implies \prod_{0 < a < p} (x - a) \equiv x^{dk} - 1 \pmod{p} \implies \\ &\implies \prod_{0 < a < p} (x - a) \equiv (x^d)^k - 1^k \pmod{p} \implies \prod_{0 < a < p} (x - a) \equiv (x^d - 1)^k \pmod{p} \implies \\ &\implies \prod_{0 < a < p} (x - a) \equiv (x^d - 1)(x^d - 1)^{k-1} \pmod{p} \end{aligned}$$

- Posto $q(x) := (x^d - 1)^{n-1}$, si ha che:

$$\begin{aligned} \prod_{0 < a < p} (x - a) &\equiv (x^d - 1)q(x) \pmod{p} \\ &\implies x - [a] \mid x^d - [1] \vee x - [a] \mid q(x), \forall 0 < a < p \end{aligned}$$

- Dunque, sia $0 < b < p$ tale che $x - [b] \mid x^d - [1]$. Ne segue che:

$$\prod_{0 < a < p, a \neq b} (x - a) \equiv q(x) \pmod{p}$$

- Per motivi di grado, ripetendo tale procedimento su $q(x)$ e i suoi fattori, otterremo esattamente d radici di $x^d - [1]$

□

Lemma 16

Dato $d \in \mathbb{N}$ tale che $d \mid p - 1$, 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 invece $d = q^k$ dove $q \in \mathbb{P}$, allora per il lemma precedente si ha che:

$$d = q^k \implies q^k \mid p - 1 \implies \begin{cases} x^{q^k} \equiv 1 \pmod{p} \text{ ha } q^k \text{ soluzioni} \\ x^{q^k-1} \equiv 1 \pmod{p} \text{ ha } q^k - 1 \text{ soluzioni} \end{cases}$$

dunque $\exists [a] \in \mathbb{Z}_p$ che è soluzione di $x^{q^k} = [1]$ ma non di $x^{q^k-1} = [1]$, implicando che:

$$o([a]) \mid q^k, o([a]) \nmid q^{k-1} \implies o([a]) = q^k$$

- Supponiamo per ipotesi induttiva di aver verificato che per tutti gli n divisori di $p - 1$ più piccoli di d che $\exists [b] \in \mathbb{Z}_p \mid o([b]) = n$
- Sia quindi $d = nq^k$ dove $q \in \mathbb{P} \mid \text{MCD}(n, q^k) = 1$. Per induzione, si ha che:

$$\exists [b], [c] \in \mathbb{Z}_p \mid o([b]) = n, o([c]) = q^k$$

- Infine, come visto nella sezione 4.11, poiché $\text{MCD}(o([b]), o([c])) = 1$ si ha che:

$$\exists a \in \mathbb{Z}_p \mid [a] = [bc] \implies o([a]) = nq^k = d$$

□

Proposizione 50

Il gruppo (\mathbb{Z}_p^*, \cdot) , dove $p \in \mathbb{P}$, è **sempre ciclico**

Dimostrazione:

- Per il lemma precedente, si ha che:

$$p - 1 \mid p - 1 \implies \exists [a] \in \mathbb{Z}_p^* \mid o([a]) = p - 1 = |\mathbb{Z}_p^*| \implies \mathbb{Z}_p^* = H([a])$$

□

8

Spazi vettoriali

Definizione 62: Spazio vettoriale

Dato un campo K , definiamo come **spazio vettoriale su K** una struttura algebrica $(V, +, \cdot)$, dove

$$+ : V \times V \rightarrow V : (u, v) \mapsto w$$

$$\cdot : K \times V \rightarrow V : (\lambda, v) \mapsto w$$

soddisfacente i seguenti assiomi:

- $(V, +)$ è un gruppo abeliano
- $\forall s, t \in K, v \in V \implies s(t \cdot v) = stv = (s \cdot t)v$ (**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**)

Inoltre, definiamo $\lambda \in K$ come **scalare** e $v \in V$ come **vettore**.

Definizione 63: Insieme di coordinate

Dato un campo K , definiamo come **insieme di coordinate** un insieme i cui elementi sono tuple di n elementi appartenenti a K :

$$K^n = K \times \dots \times K = \{(t_1, \dots, t_n) \mid t_1, \dots, t_n \in K\}$$

Proposizione 51: Spazio di coordinate

La struttura $(K^n, +, \cdot)$ è uno **spazio vettoriale**, dove l'**addizione tra vettori** e il **prodotto per scalare** sono definite come:

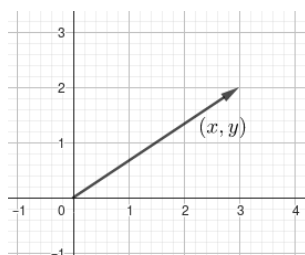
$$\begin{aligned} v &:= (t_1, \dots, t_n) \in K^n \\ w &:= (s_1, \dots, s_n) \in K^n \end{aligned} \implies v + w := (t_1 + s_1, \dots, t_n + s_n) \in K^n$$

$$\lambda \in K, v := (t_1, \dots, t_n) \in K^n \implies \lambda v := (\lambda t_1, \dots, \lambda t_n) \in K^n$$

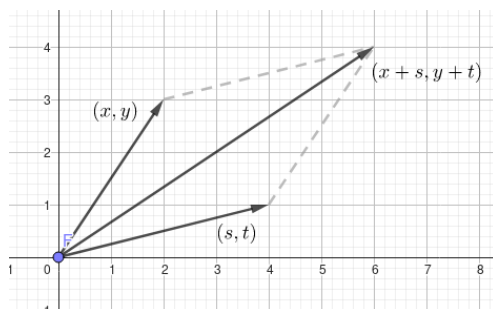
(dimostrazione omessa)

Interpretazione geometrica:

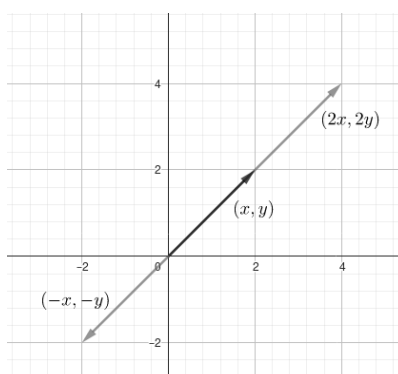
- Dato lo spazio di coordinate \mathbb{R}^2 e un vettore $v := (x, y) \in \mathbb{R}^2$, possiamo rappresentare tale vettore come:



- Preso $w := (s, t) \in \mathbb{R}^2$, la somma vettoriale $v + w$ corrisponde al classico *metodo del parallelogramma* utilizzato in fisica elementare:



- Preso $\lambda \in \mathbb{R}$, il prodotto per scalare $\lambda \cdot v$ ha la stessa direzione del vettore v , ma con lunghezza aumentata o diminuita e verso uguale o invertito



Osservazione 51

Dato uno spazio vettoriale V su un campo K , si ha che:

- $\forall \lambda \in K \implies \lambda \cdot 0_V = 0_V$
- $\forall v \in V \implies 0 \cdot v = 0_V$

Dato $0_V = (0, \dots, 0) \in V$ è detto **vettore nullo**, ossia l'elemento neutro di V , e dove 0 è l'elemento neutro di K

Dimostrazione:

- Dato $\lambda \in K$, si ha che:

$$\lambda \cdot 0_V = (\lambda \cdot 0, \dots, \lambda \cdot 0) = (0, \dots, 0) = 0_V$$

- Dato $v = (t_1, \dots, t_n) \in V$, si ha che:

$$0 \cdot v = (0 \cdot t_1, \dots, 0 \cdot t_n) = (0, \dots, 0) = 0_V$$

□

Definizione 64: Sottospazio vettoriale

Dato un spazio vettoriale V su K , definiamo $W \subseteq V$ come **sottospazio vettoriale** di V su K se:

- $(W, +) \leq (V, +)$
- $w \in W, \lambda \in K \implies \lambda w \in W$

Esempi:

- $\mathbb{Z}^n \subseteq \mathbb{R}^n$ non è sottospazio vettoriale di \mathbb{R}^n poiché non vale la seconda condizione
- $\mathbb{R}_{\geq 0}^n \subseteq \mathbb{R}^n$ non è sottospazio vettoriale di \mathbb{R}^n poiché non vale nessuna delle due condizioni

8.1 Span, Generatori e Indipendenza lineare

Definizione 65: 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:

$$\text{span}(v_1, \dots, v_n) = \{\lambda_1 v_1 + \dots + \lambda_n v_n \mid \lambda_1, \dots, \lambda_n \in K\}$$

Dimostrazione:

- $0_V = 0 \cdot v_1 + \dots + 0 \cdot v_n \in \text{span}(v_1, \dots, v_n)$
- $v, w \in \text{span}(v_1, \dots, v_n) \implies v + w = \lambda_1 v_1 + \dots + \lambda_n v_n + \mu_1 v_1 + \dots + \mu_n v_n = (\lambda_1 + \mu_1)v_1 + \dots + (\lambda_n + \mu_n)v_n \implies v + w \in \text{span}(v_1, \dots, v_n)$
- $v \in \text{span}(v_1, \dots, v_n) \implies -v = (-\lambda_1)v_1 + \dots + (-\lambda_n)v_n \in \text{span}(v_1, \dots, v_n)$
- $v \in \text{span}(v_1, \dots, v_n), c \in K \implies cv = (c\lambda_1)v_1 + \dots + (c\lambda_n)v_n \in \text{span}(v_1, \dots, v_n)$

□

Definizione 66: Insieme di generatori

Dato uno spazio vettoriale V su K , definiamo i vettori $v_1, \dots, v_n \neq 0_V \in V$ come un **insieme di generatori di V** se e solo se ogni vettore di V può essere espresso come una combinazione lineare di v_1, \dots, v_n :

$$\forall v \in V, \exists \lambda_1, \dots, \lambda_n \mid v = \lambda_1 v_1 + \dots + \lambda_n v_n$$

o analogamente se e solo se:

$$V = \text{span}(v_1, \dots, v_n)$$

Dimostrazione:

- Poiché $v_1, \dots, v_n \in V$, per definizione stessa si ha sempre che $\text{span}(v_1, \dots, v_n) \subseteq V$
- Dunque, affinché le due definizioni siano equivalenti è sufficiente che:

$$\forall v \in V, \exists \lambda_1, \dots, \lambda_n \mid v = \lambda_1 v_1 + \dots + \lambda_n v_n \iff V \subseteq \text{span}(v_1, \dots, v_n)$$

□

Definizione 67: Indipendenza lineare

Dato uno spazio vettoriale V su K , definiamo i vettori $v_1, \dots, v_n \neq 0_V \in V$ come **linearmente indipendenti** se e solo 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**

Osservazione 52

Sia V uno spazio vettoriale. Dati i vettori $v_1, \dots, v_n \neq 0_V \in V$, si ha che:

$$v_1, \dots, v_n \text{ lin. ind.} \iff v_1, \dots, v_{n-1} \text{ lin. ind.} \wedge v_n \notin \text{span}(v_1, \dots, v_{n-1})$$

Dimostrazione:

- Nel caso in cui v_1, \dots, v_n siano linearmente indipendenti, si ha che:

$$\lambda_1 v_1 + \dots + \lambda_{n-1} v_{n-1} + \lambda_n v_n = 0_V \iff \lambda_1 = \dots = \lambda_{n-1} = \lambda_n = 0$$

da cui ne segue automaticamente che:

$$\lambda_1 v_1 + \dots + \lambda_{n-1} v_{n-1} = 0_V \iff \lambda_1 = \dots = \lambda_{n-1} = 0$$

dunque anche v_1, \dots, v_{n-1} sono linearmente indipendenti

- Supponiamo quindi che $v_n \in \text{span}(v_1, \dots, v_{n-1})$, implicando che:

$$\mu_1 v_1 + \dots + \mu_{n-1} v_{n-1} = v_n \iff \mu_1 v_1 + \dots + \mu_{n-1} v_{n-1} - v_n = 0_V \iff$$

$$\iff \mu_1 v_1 + \dots + \mu_{n-1} v_{n-1} + (-1)v_n = 0_V$$

dunque v_1, \dots, v_n sono linearmente dipendenti. Per contronominale, quindi, si ha che:

$$v_1, \dots, v_n \text{ lin. indipendenti} \implies v_n \notin \text{span}(v_1, \dots, v_{n-1})$$

- Viceversa, supponiamo per assurdo che $v_n \notin \text{span}(v_1, \dots, v_n)$ e che $\exists \lambda_n \neq 0 \mid \lambda_1 v_1 + \dots + \lambda_n v_n = 0_V$. Ne segue che

$$\lambda_1 v_1 + \dots + \lambda_n v_n = 0_V \implies \lambda_n v_n = -\lambda_1 v_1 - \dots - \lambda_{n-1} v_{n-1} \implies$$

$$\implies v_n = (-\lambda_n^{-1} \lambda_1) v_1 + \dots + (-\lambda_n^{-1} \lambda_{n-1}) v_{n-1} \implies v_n \in \text{span}(v_1, \dots, v_{n-1})$$

contraddicendo quindi l'ipotesi $v_n \notin \text{span}(v_1, \dots, v_n)$, implicando quindi che l'unica possibilità sia $\lambda_n = 0$.

- Di conseguenza, nel caso in cui v_1, \dots, v_{n-1} siano linearmente indipendenti e $v_n \notin \text{span}(v_1, \dots, v_n)$, otteniamo che:

$$\lambda_1 v_1 + \dots + \lambda_{n-1} v_{n-1} + \lambda_n v_n = 0_V \iff \lambda_1 v_1 + \dots + \lambda_{n-1} v_{n-1} + 0 \cdot v_n = 0_V \iff$$

$$\iff \lambda_1 v_1 + \dots + \lambda_{n-1} v_{n-1} = 0_V \iff \lambda_1 = \dots = \lambda_{n-1} = 0 = \lambda_n$$

dunque v_1, \dots, v_n sono linearmente indipendenti

□

Proposizione 52: Estensione a generatore

Dati i vettori **linearmente indipendenti** $v_1, \dots, v_k \in \text{span}(w_1, \dots, w_n)$, allora:

- $k \leq n$
- $\exists v_{k+1}, \dots, v_n \in \text{span}(w_1, \dots, w_n) \mid \text{span}(v_1, \dots, v_n) = \text{span}(w_1, \dots, w_n)$ dove v_1, \dots, v_n sono linearmente indipendenti

Dimostrazione:

- Dato $v_1 \neq 0 \in \text{span}(w_1, \dots, w_n)$, il quale è ovviamente linearmente indipendente con se stesso, si ha che:

$$\exists \lambda_i \neq 0 \in K, i \in [1, n] \mid v = \lambda_1 w_1 + \dots + \lambda_n w_n \neq 0_V$$

- A meno di riordinare i termini, assumiamo che $\lambda_1 \neq 0$

$$\begin{aligned} v = \lambda_1 w_1 + \dots + \lambda_n w_n &\implies \lambda_1 w_1 = v - \lambda_2 w_2 - \dots - \lambda_n w_n \implies \\ \implies w_1 &= (\lambda_1^{-1})v + (-\lambda_1^{-1}\lambda_2)w_2 - \dots + (-\lambda_1^{-1}\lambda_n)w_n \implies w_1 \in \text{span}(v_1, w_2, \dots, w_n) \end{aligned}$$

- Poiché $w_1 = \mu_1 v_1 + \mu_2 w_2 + \dots + \mu_n w_n \in \text{span}(v_1, w_2, \dots, w_n)$, ne segue che:

$$\begin{aligned} u \in \text{span}(w_1, \dots, w_n) &\iff u = \lambda_1 w_1 + \lambda_2 w_2 + \dots + \lambda_n w_n = \\ &= \lambda_1(\mu_1 v_1 + \mu_2 w_2 + \dots + \mu_n w_n) + \lambda_2 w_2 + \dots + \lambda_n w_n = \\ &= (\lambda_1 \mu_1) v_1 + (\lambda_1 \lambda_2 \mu_2) w_2 + \dots + (\lambda_1 \lambda_n \mu_n) w_n \iff u \in \text{span}(v_1, w_2, \dots, w_n) \end{aligned}$$

dunque si ha che $\text{span}(v_1, w_2, \dots, w_n) = \text{span}(w_1, \dots, w_n)$

- Supponiamo quindi induttivamente che dati $v_1, \dots, v_i \in \text{span}(w_1, \dots, w_n)$ linearmente indipendenti, dove $i \leq n$, si ha che:

$$\text{span}(v_1, \dots, v_i, w_{i+1}, \dots, w_n) = \text{span}(w_1, \dots, w_n)$$

- Preso $v_{i+1} = \mu_1 v_1 + \dots + \mu_i v_i + \lambda_{i+1} w_{i+1} + \dots + \lambda_n w_n \in \text{span}(v_1, \dots, v_i, w_{i+1}, \dots, w_n)$, supponiamo per assurdo che $\lambda_{i+1}, \dots, \lambda_n = 0$, implicando che:

$$\begin{aligned} v_{i+1} &= \mu_1 v_1 + \dots + \mu_i v_i + \lambda_{i+1} w_{i+1} + \dots + \lambda_n w_n \implies \\ \implies v_{i+1} &= \mu_1 v_1 + \dots + \mu_i v_i + 0 \cdot w_{i+1} + \dots + 0 \cdot w_n \implies \\ \implies v_{i+1} &= \mu_1 v_1 + \dots + \mu_i v_i \implies 0_V = (-1)v_{i+1} + \mu_1 v_1 + \dots + \mu_i v_i \end{aligned}$$

contraddicendo l'ipotesi per cui v_1, \dots, v_k siano linearmente indipendenti, dunque l'unica possibilità è

$$\exists \lambda_j \neq 0, j \in [i+1, n] \mid v_{i+1} = \mu_1 v_1 + \dots + \mu_i v_i + \lambda_{i+1} w_{i+1} + \dots + \lambda_n w_n \neq 0_V \iff$$

- A meno di riordinare i termini, assumiamo che $\lambda_{i+1} \neq 0$

$$\begin{aligned} v_{i+1} &= \mu_1 v_1 + \dots + \mu_i v_i + \lambda_{i+1} w_{i+1} + \dots + \lambda_n w_n \implies \\ \implies \lambda_{i+1} w_{i+1} &= v_{i+1} - \mu_1 v_1 - \dots - \mu_i v_i - \lambda_{i+2} w_{i+2} - \dots - \lambda_n w_n \implies \\ w_{i+1} &= (\lambda_{i+1}^{-1})v_{i+1} + (-\lambda_{i+1}^{-1}\mu_1)v_1 + \dots + (-\lambda_{i+1}^{-1}\mu_i)v_i + (-\lambda_{i+1}^{-1}\lambda_{i+2})w_{i+2} + \dots + (-\lambda_{i+1}^{-1}\lambda_n)w_n \\ \implies w_{i+1} &\in \text{span}(v_1, \dots, v_i, v_{i+1}, w_{i+2}, \dots, w_n) \end{aligned}$$

- Poiché $w_{i+1} = \mu_1 v_1 + \dots + \mu_{i+1} v_{i+1} + \mu_{i+2} w_{i+2} + \dots + \mu_n w_n \in \text{span}(v_1, \dots, v_{i+1}, w_{i+2}, \dots, w_n)$, procedendo analogamente al caso base si ha che::

$$u \in \text{span}(w_1, \dots, w_n) \iff u \in \text{span}(v_1, \dots, v_{i+1}, w_{i+2}, \dots, w_n)$$

dunque si ha che $\text{span}(w_1, \dots, w_n) = \text{span}(v_1, \dots, v_{i+1}, w_{i+2}, \dots, w_n)$, implicando quindi per induzione che

$$\text{span}(w_1, \dots, w_n) = \text{span}(v_1, \dots, v_n)$$

- Supponiamo per assurdo che vi possano essere $k > n$ vettori linearmente indipendenti, dunque che $\exists v_{n+1} \in \text{span}(w_1, \dots, w_n) \mid v_1, \dots, v_n, v_{n+1}$ linearmente indipendenti. Poiché $\text{span}(w_1, \dots, w_n) = \text{span}(v_1, \dots, v_n)$, ne segue che:

$$v_{n+1} \in \text{span}(w_1, \dots, w_n) = \text{span}(v_1, \dots, v_n)$$

contraddicendo l'ipotesi per cui v_1, \dots, v_n, v_k siano indipendenti, dunque l'unica possibilità è che i vettori linearmente indipendenti siano $k \leq n$

□

8.2 Base e Dimensione

Definizione 68: Base

Dato uno spazio vettoriale V su K , definiamo i vettori $v_1, \dots, v_n \neq 0_V \in V$ come una **base** se e solo se sono un **insieme di generatori** e **linearmente indipendenti**

Osservazione 53

Dato uno spazio vettoriale V , si ha che:

$$v_1, \dots, v_n \text{ base di } V \iff \forall v \in V, \exists! \lambda_1, \dots, \lambda_n \mid v = \lambda_1 v_1 + \dots + \lambda_n v_n$$

Inoltre, chiamiamo tali unici scalari come **coordinate di v in base v_1, \dots, v_n**

Dimostrazione:

- Nel caso in cui $\forall v \in V, \exists! \lambda_1, \dots, \lambda_n \mid v = \lambda_1 v_1 + \dots + \lambda_n v_n$, per definizione stessa di vettori generatori si ha che v_1, \dots, v_n sono generatori di V
- Inoltre, poiché tali coordinate sono uniche, ne segue naturalmente che:

$$\exists! \lambda_1 = \dots = \lambda_n = 0 \in K \mid \lambda_1 v_1 + \dots + \lambda_n v_n = 0_V$$

dunque v_1, \dots, v_n sono linearmente indipendenti

- Viceversa, se $v_1, \dots, v_n \in V$ sono una base di V , si ha che:

$$V = \text{span}(v_1, \dots, v_n) = \{\lambda_1 v_1 + \dots + \lambda_n v_n \mid \lambda_1, \dots, \lambda_n \in K\}$$

- Dato $v \in V$, supponiamo per assurdo che esistano due combinazioni lineari di v_1, \dots, v_n tali che

$$\begin{aligned} \mu_1 v_1 + \dots + \mu_n v_n = v = \lambda_1 v_1 + \dots + \lambda_n v_n &\implies \mu_1 v_1 + \dots + \mu_n v_n = \lambda_1 v_1 + \dots + \lambda_n v_n \implies \\ \implies \mu_1 v_1 + \dots + \mu_n v_n - \lambda_1 v_1 - \dots - \lambda_n v_n = 0_V &\implies (\lambda_1 - \mu_1)v_1 + \dots + (\lambda_n - \mu_n)v_n = 0_V \end{aligned}$$

- Poiché v_1, \dots, v_n sono linearmente indipendenti, si ha che:

$$\begin{aligned} (\lambda_1 - \mu_1)v_1 + \dots + (\lambda_n - \mu_n)v_n = 0_V &\iff (\lambda_1 - \mu_1) = \dots = (\lambda_n - \mu_n) = 0 \iff \\ &\iff \lambda_1 = \mu_1, \dots, \lambda_n = \mu_n \end{aligned}$$

□

Osservazione 54: Base canonica

Dato uno spazio di coordinate K^n , definiamo i vettori $e_1, \dots, e_n \in K^n$ come **base canonica di K^n** , dove:

$$e_i = (a_1, \dots, a_n) \mid \begin{cases} a_j = 0 & \text{se } j \neq i \\ a_j = 1 & \text{se } j = i \end{cases}$$

Dimostrazione:

- Dati $e_1, \dots, e_n \in K^n$ definiti come:

$$\begin{aligned} - e_1 &= (1, 0, 0, \dots, 0, 0) \\ - e_2 &= (0, 1, 0, \dots, 0, 0) \\ - &\vdots \\ - e_n &= (0, 0, 0, \dots, 0, 1) \end{aligned}$$

- Si ha che:

$$\begin{aligned} v = (t_1, \dots, t_n) \in K^n &\iff v = (t_1, \dots, 0) + \dots + (0, \dots, t_n) \\ &\iff v = t_1 e_1 + \dots + t_n e_n \in \text{span}(e_1, \dots, e_n) \end{aligned}$$

dunque tali vettori sono generatori poiché $K^n = \text{span}(e_1, \dots, e_n)$

- Analogamente, si ha che:

$$\begin{aligned} \lambda_1 e_1 + \dots + \lambda_n e_n = (0, \dots, 0) &\iff (\lambda_1, 0, \dots, 0) + \dots + (0, 0, \dots, \lambda_n) = (0, \dots, 0) \\ (\lambda_1, \lambda_2, \dots, \lambda_n) = (0, \dots, 0) &\iff \lambda_1 = \dots = \lambda_n = 0 \end{aligned}$$

dunque tali vettori sono anche linearmente indipendenti, costituendo quindi una base di K^n

□

Teorema 21: Teorema della cardinalità delle basi

Sia V uno spazio vettoriale. Se v_1, \dots, v_n e w_1, \dots, w_m sono due basi di V , si ha necessariamente che $n = m$.

Dunque tutte le basi di uno spazio vettoriale hanno la **stessa cardinalità**

Dimostrazione:

- Poiché i due insiemi di vettori sono entrambi base di V , 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, ne segue che $n \leq m$
- Analogamente, poiché i vettori $w_1, \dots, w_m \in V = \text{span}(v_1, \dots, v_n)$ sono linearmente indipendenti, ne segue che $m \leq n$
- Dunque, l'unica possibilità è che $n = m$

□

Definizione 69: Dimensione di uno spazio vettoriale

Dato uno spazio vettoriale V , definiamo come **dimensione di V** , indicata come $\dim(V)$ la **cardinalità di una sua qualsiasi base** (poiché ogni base di V ha la stessa cardinalità).

Nel caso in cui non esista un insieme finito di generatori di V , definiamo la sua dimensione come **infinita**.

Esempi:

- Lo spazio di coordinate K^n e la sua base canonica e_1, \dots, e_n , si ha che:

$$\dim(K^n) = n$$

- Lo spazio vettoriale $K[x]$ 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 $1, x, x^2, \dots$, dunque non esiste un insieme finito di generatori di $K[X]$

- Lo spazio vettoriale $K^S := \{f : S \rightarrow K\}$ ha dimensione finita se e solo se S ha cardinalità finita

Lemma 17: Estensione a base

Sia V uno spazio vettoriale dove $\dim(V) = n$. Dati i vettori **linearmente indipendenti** $v_1, \dots, v_k \in V$, dove $k < n$ allora:

$$\exists v_{k+1}, \dots, v_n \in V \mid v_1, \dots, v_n \text{ sono base di } V$$

Dimostrazione:

- Poiché $\dim(V) = n$, sia w_1, \dots, w_n una base qualsiasi di V . Per dimostrazione precedente, dato $k < n$ si ha che:

$$\exists v_{k+1}, \dots, v_n \in V \mid \text{span}(v_1, \dots, v_n) = \text{span}(w_1, \dots, w_n) = V$$

dove v_1, \dots, v_n sono anche linearmente indipendenti, dunque costituiscono una base di V

□

Lemma 18: Riduzione a base

Sia V uno spazio vettoriale dove $\dim(V) = n$. Dato l'**insieme di generatori** v_1, \dots, v_k di V , dove $k \geq n$ allora:

$$\exists v_{i_1}, \dots, v_{i_n} \in \{v_1, \dots, v_k\} \mid v_{i_1}, \dots, v_{i_n} \text{ sono base di } V$$

Dimostrazione:

- Dati v_1, \dots, v_m generatori di V , assumiamo che $\exists v_{k_1} \neq 0 \in \{v_1, \dots, v_m\}$, il quale è ovviamente linearmente indipendente con se stesso
- Poiché $\text{span}(v_{i_1}) \subsetneq \text{span}(v_1, \dots, v_m) = W$, allora

$$\exists v_{i_2} \in \{v_1, \dots, v_m\} \mid v_{i_2} \notin \text{span}(v_{i_1}) \iff v_{i_1}, v_{i_2} \text{ lin. ind.}$$

- Ripetendo tale procedimento n , estendiamo l'insieme v_{i_1}, \dots, v_{i_n} di vettori linearmente indipendenti fino a che essi non siano generatori di V :

$$\text{span}(v_{i_1}, \dots, v_{i_n}) = \text{span}(v_1, \dots, v_m) = V$$

dunque v_{i_1}, \dots, v_{i_n} sono una base di V

□

Proposizione 53

Sia V uno spazio vettoriale dove $\dim(V) = n$. Dati i vettori $v_1, \dots, v_n \in V$, si ha che:

$$v_1, \dots, v_n \text{ lin. ind.} \iff v_1, \dots, v_n \text{ generatori}$$

Dimostrazione:

- Supponiamo per assurdo che $v_1, \dots, v_n \in V$ siano linearmente indipendenti ma che non siano generatori di V , dunque $\text{span}(v_1, \dots, v_n) \subsetneq V$. Ne segue che:

$$\exists v_{n+1} \in W \mid v_{n+1} \notin \text{span}(v_1, \dots, v_n) \implies v_1, \dots, v_{n+1} \text{ lin. ind.}$$

contraddicendo la condizione per cui $\dim(V) = n$ implica che non possano esistere più di n vettori linearmente indipendenti (sezione 8.1), dunque l'unica possibilità è che v_1, \dots, v_n siano anche generatori di V

- Viceversa, supponiamo per assurdo che v_1, \dots, v_n siano generatori di V ma non linearmente indipendenti. Ne segue che:

$$\begin{aligned} \exists \lambda_i \neq 0 \in K, i \in [1, n] \mid \lambda_1 v_1 + \dots + \lambda_i v_i + \dots + \lambda_n v_n = 0_V &\implies \\ v_i = (\lambda_i^{-1} \lambda_1) v_1 + \dots + (\lambda_i^{-1} \lambda_n) v_n = 0_V &\implies v_i \in \text{span}(v_1, \dots, \hat{v}_i, \dots, v_n) \end{aligned}$$

dove \hat{v}_i indica che tale elemento è escluso

- A questo punto, si ha che:

$$u \in \text{span}(v_1, \dots, v_n) \iff u \in \text{span}(v_1, \dots, \hat{v}_i, \dots, v_n)$$

da cui otteniamo che:

$$W = \text{span}(v_1, \dots, v_n) = \text{span}(v_1, \dots, \hat{v}_i, \dots, v_n)$$

contraddicendo la condizione per cui $\dim(V) = n$ implica che non possano esistere meno di n generatori di V , dunque l'unica possibilità è che v_1, \dots, v_n siano anche linearmente indipendenti

□

8.2.1 Formula di Grassman

Teorema 22: Formula di Grassmann

Dato uno spazio vettoriale W su K e dati due sottospazi $U, V \subseteq W$, i seguenti insiemi:

$$U + V := \{u + v \mid u \in U, v \in V\}$$

$$U \cap V := \{w \mid w \in U, w \in V\}$$

sono due sottospazi di W , dove:

$$\dim(U + V) = \dim(U) + \dim(V) - \dim(U \cap V)$$

Dimostrazione:

- Dati: $k := \dim(U \cap V)$, $m := \dim(U)$, $n := \dim(V)$, siano:

- w_1, \dots, w_k una base di $U \cap V$
- $\mathcal{B}_1 := w_1, \dots, w_k, u_{k+1}, \dots, u_m$ una base di U
- $\mathcal{B}_2 := w_1, \dots, w_k, v_{k+1}, \dots, v_n$ una base di V

- Consideriamo quindi il seguente insieme di vettori:

$$\mathcal{B}_1 \cup \mathcal{B}_2 = w_1, \dots, w_k, u_{k+1}, \dots, u_m, v_{k+1}, \dots, v_n$$

- Dati $u \in \text{span}(\mathcal{B}_1) = U$ e $v \in \text{span}(\mathcal{B}_2) = V$, dove

$$u = \sum_{i=1}^k \lambda_i w_i + \sum_{j=k+1}^m \lambda_j u_j \quad v = \sum_{i=1}^k \lambda_i w_i + \sum_{j=k+1}^n \lambda_j v_j$$

si ha che :

$$\begin{aligned} u + v \in U + V &\iff u + v = \sum_{i=1}^k \lambda_i w_i + \sum_{j=k+1}^m \lambda_j u_j + \sum_{i=1}^k \mu_i w_i + \sum_{j=k+1}^n \mu_j v_j \iff \\ &\iff u + v = \sum_{i=1}^k (\lambda_i + \mu_i) w_i + \sum_{j=k+1}^m \lambda_j u_j + \sum_{j=k+1}^n \mu_j v_j \iff u + v \in \text{span}(\mathcal{B}_1 \cup \mathcal{B}_2) \end{aligned}$$

dunque $\mathcal{B}_1 \cup \mathcal{B}_2$ sono generatori di $U + V$

- Consideriamo quindi $0_W \in U + V$ scritto come combinazione lineare di tale base

$$\sum_{i=1}^k \beta_i w_i + \sum_{j=k+1}^m \gamma_j u_j + \sum_{h=k+1}^n \eta_h v_h = 0_W$$

- Posti:

$$a := \sum_{i=1}^k \beta_i w_i \quad b := \sum_{j=k+1}^m \gamma_j u_j \quad c := \sum_{h=k+1}^n \eta_h v_h$$

si ha che:

$$a + b + c = 0_W \iff b = -a - c \implies b \in \text{span}(\mathcal{B}_2) = V$$

inoltre, poiché $b \in \text{span}(u_{k+1}, \dots, u_m) \subsetneq U \implies b \in U$, ne segue che $b \in U \cap V$

- Di conseguenza, si ha che:

$$\begin{aligned} \begin{cases} b := \sum_{j=k+1}^m \gamma_j u_j \\ b \in U \cap V \iff b = \sum_{t=0}^k \alpha_t w_t \end{cases} &\implies \sum_{j=k+1}^m \gamma_j u_j = \sum_{t=0}^k \alpha_t w_t \implies \\ &\implies \sum_{t=0}^k \alpha_t w_t - \sum_{j=k+1}^m \gamma_j u_j = 0_W \end{aligned}$$

- Poiché $\mathcal{B}_1 = w_1, \dots, w_k, u_{k+1}, \dots, u_m$ è una base di U , dunque sono vettori linearmente indipendenti, ne segue che:

$$\sum_{t=0}^k \alpha_t w_t - \sum_{j=k+1}^m \gamma_j u_j = 0_W \iff \alpha_1 = \dots = \alpha_k = \gamma_{k+1} = \dots = \gamma_m = 0$$

- In particolare, quindi, otteniamo che $\gamma_{k+1} = \dots = \gamma_m = 0 \implies b = 0_W$, da cui traiamo che:

$$a + b + c = 0_W \implies a + 0_W + c = 0_W \implies a + c = 0_W$$

- A questo punto, poiché:

$$a + c = 0_W \implies \sum_{i=1}^k \beta_i w_i + \sum_{h=k+1}^n \eta_h v_h = 0_W$$

e poiché $\mathcal{B}_2 := w_1, \dots, w_k, v_{k+1}, \dots, v_n$ è una base di V , dunque sono vettori linearmente indipendenti, ne segue che:

$$\sum_{i=1}^k \beta_i w_i + \sum_{h=k+1}^n \eta_h v_h = 0_W \iff \beta_1 = \dots = \beta_k = \eta_{k+1} = \dots = \eta_n = 0$$

concludendo quindi che i vettori $\mathcal{B}_1 \cup \mathcal{B}_2 = w_1, \dots, w_k, u_{k+1}, \dots, u_m, v_{k+1}, \dots, v_n$ siano anche linearmente indipendenti, costituendo quindi una base di $U + V$

- Infine, si ha che:

$$\begin{aligned} \dim(U + V) &= \dim(\text{span}(w_1, \dots, w_k, u_{k+1}, \dots, u_m, v_{k+1}, \dots, v_n)) = \\ &= k + (m - k) + (n - k) = m + n - k = \dim(U) + \dim(V) - \dim(U \cap V) \end{aligned}$$

□

8.3 Trasformazioni lineari

Definizione 70: 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:

- $\forall v, v' \in V, f(v + v') = f(v) + f(v')$
- $\forall \lambda \in K, v \in V, f(\lambda v) = \lambda f(v)$

Lemma 19

Dato uno spazio vettoriale V si ha che:

$$\dim(V) = n \implies V \cong K^n$$

Dimostrazione:

- Dato $\dim(V) = n$, sia v_1, \dots, v_n una base di V . Definiamo la funzione

$$\varphi : K^n \rightarrow V : (t_1, \dots, t_n) \mapsto (t_1 v_1 + \dots + t_n v_n)$$

dunque φ mappa ogni vettore di K^n ad una combinazione lineare di V

- Poiché:

$$v_1, \dots, v_n \text{ base di } V \iff \forall v \in V, \exists! \lambda_1, \dots, \lambda_n \in K \mid v = \lambda_1 v_1 + \dots + \lambda_n v_n$$

e poiché $\dim(K^n) = n$, la funzione φ risulta essere automaticamente biettiva:

$$\forall v := \varphi(u) \in V, \exists! u := (t_1, \dots, t_n) \in K^n \mid \varphi(u) = t_1 v_1 + \dots + t_n v_n$$

- Dati quindi $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in K^n$, si ha che:

$$\varphi(x+y) = (x_1+y_1)v_1 + \dots + (x_n+y_n)v_n = x_1 v_1 + \dots + x_n v_n + y_1 v_1 + \dots + y_n v_n = \varphi(x) + \varphi(y)$$

- Dato invece $\lambda \in K$, si ha che:

$$\varphi(\lambda v) = \lambda x_1 v_1 + \dots + \lambda x_n v_n = \lambda(x_1 v_1 + \dots + x_n v_n) = \lambda \varphi(x)$$

- Dunque, concludiamo che φ sia un isomorfismo e di conseguenza che:

$$V \cong K^n$$

□

Teorema 23: Teorema delle dimensioni

Dati due spazi vettoriali V e W definiti sullo stesso K , si ha che:

$$V \cong W \iff \dim(V) = \dim(W)$$

Dimostrazione:

- Nel caso in cui $\dim(V) = \dim(W) = n$ dove $n \in \mathbb{N}$, per il lemma precedente si ha che:

$$\begin{aligned} \dim(V) = n, \dim(W) = n &\implies V \cong K^n, W \cong K^n \implies \\ &\implies V \cong K^n, K^n \cong W \implies V \cong W \end{aligned}$$

- Viceversa, supponiamo che $V \cong W$, dove f è l'isomorfismo che rende V isomorfo a W . Sia inoltre v_1, \dots, v_n la base di V .
- Poiché f è un morfismo suriettivo, si ha che:

$$\begin{aligned} \forall w \in W, \exists v \in V \mid w = f(v) = f(\lambda_1 v_1 + \dots + \lambda_n v_n) = \\ f(\lambda_1 v_1) + \dots + f(\lambda_n v_n) = \lambda_1 f(v_1) + \dots + \lambda_n f(v_n) \end{aligned}$$

dunque, poiché anche $f(v_1), \dots, f(v_n)$ sono vettori di W , ne segue che $f(v_1), \dots, f(v_n)$ siano generatori di W

- Inoltre, poiché f è iniettiva se e solo se $\ker(f) = \{0_V\}$ e poiché ne segue che:

$$\begin{aligned} \mu_1 f(v_1) + \dots + \mu_n f(v_n) = 0_W &\iff f(\mu_1 v_1) + \dots + f(\mu_n v_n) = 0_W \iff \\ &\iff f(\mu_1 v_1 + \dots + \mu_n v_n) = 0_W \iff \mu_1 v_1 + \dots + \mu_n v_n = 0_V \iff \mu_1 = \dots = 0 \end{aligned}$$

dunque $f(v_1), \dots, f(v_n)$ sono anche linearmente indipendenti, costituendo quindi una base di W , implicando quindi che $\dim(W) = n = \dim(V)$

□

Definizione 71: Spazio quoziente

Dato uno spazio vettoriale V e un sottospazio $W \subseteq V$, la struttura $(V/W, +, \cdot)$ è uno spazio vettoriale, detto **spazio quoziente**, dove la somma è definita come $[v] + [v'] = [v + v']$ e il prodotto per scalare è definito come $\lambda[x] = [\lambda x]$.

Dimostrazione:

- La dimostrazione della buona definizione della somma risulta analoga a quella del normale gruppo quoziente
- Dimostriamo quindi che il prodotto per scalare sia ben definito

$$[v] = [v'] \implies v' - v \in W \implies \lambda(v' - v) \in W \implies [\lambda v] = [\lambda v']$$

- La dimostrazione di $(V/W, +, \cdot)$ spazio vettoriale viene omessa poiché banale

□

Teorema 24: Dimensione di uno spazio quoziente

Dato uno spazio vettoriale V e un sottospazio $W \subseteq V$, si verifica che

$$\dim(V/W) = \dim(V) - \dim(W)$$

Dimostrazione:

- Siano $n := \dim(V)$, $k := \dim(W)$ e w_1, \dots, w_k una base di W .

- Poiché $k \leq n$, è possibile estendere con $n - k$ vettori di V l'insieme w_1, \dots, w_k fino a formare una base di V :

$$\exists v_{k+1}, \dots, v_n \in V \mid w_1, \dots, w_k, v_{k+1}, \dots, v_n \text{ base di } V$$

- Dato $v \in V = \text{span}(w_1, \dots, w_k, v_{k+1}, \dots, v_n)$, si ha che:

$$\begin{aligned} v &= \lambda_1 w_1 + \dots + \lambda_k w_k + \lambda_{k+1} v_{k+1} + \dots + \lambda_n v_n \implies \\ \implies [v] &= \lambda_1 [w_1] + \dots + \lambda_k [w_k] + \lambda_{k+1} [v_{k+1}] + \dots + \lambda_n [v_n] \end{aligned}$$

- Poiché:

$$w_1, \dots, w_k \in W \iff w_1 \sim 0_V, \dots, w_k \sim 0_V \iff [0_V] = [w_1] = \dots = [w_k]$$

si ha che:

$$\begin{aligned} [v] &= \lambda_1 [w_1] + \dots + \lambda_k [w_k] + \lambda_{k+1} [v_{k+1}] + \dots + \lambda_n [v_n] \iff \\ \iff [v] &= \lambda_1 [0_V] + \dots + \lambda_k [0_V] + \lambda_{k+1} [v_{k+1}] + \dots + \lambda_n [v_n] \iff \\ \iff [v] &= \lambda_{k+1} [v_{k+1}] + \dots + \lambda_n [v_n] \end{aligned}$$

dunque, $[v_{k+1}], \dots, [v_n]$ sono generatori di V/W

- Preso $[0_V] \in V/W$, si ha che:

$$\begin{aligned} [0_V] &= \lambda_{k+1} [v_{k+1}] + \dots + \lambda_n [v_n] \iff [0_V] = [\lambda_{k+1} v_{k+1} + \dots + \lambda_n v_n] \iff \\ \iff u &:= \lambda_{k+1} v_{k+1} + \dots + \lambda_n v_n \in W \end{aligned}$$

- Poiché anche w_1, \dots, w_k è base di W e poiché $u \in W$, si ha che:

$$\begin{aligned} u &= \lambda_{k+1} v_{k+1} + \dots + \lambda_n v_n = \mu_1 w_1 + \dots + \mu_k w_k \iff \\ \iff \lambda_{k+1} v_{k+1} + \dots + \lambda_n v_n &= \mu_1 w_1 + \dots + \mu_k w_k \iff \\ \iff \mu_1 w_1 + \dots + \mu_k w_k - \lambda_{k+1} v_{k+1} - \dots - \lambda_n v_n &= 0_V \iff \\ \iff \mu_1 = \dots = \mu_k = \lambda_{k+1} = \dots = \lambda_n &= 0 \end{aligned}$$

dato che $w_1, \dots, w_k, v_{k+1}, \dots, v_n$ sono base di V , dunque linearmente indipendenti.

- In particolare, quindi, dati $\lambda_{k+1} = \dots = \lambda_n = 0$ ne segue che:

$$[0_V] = \lambda_{k+1} [v_{k+1}] + \dots + \lambda_n [v_n] \iff \lambda_{k+1} = \dots = \lambda_n = 0$$

implicando che anche $[v_{k+1}], \dots, [v_n]$ siano linearmente indipendenti, costituendo quindi base di V/W , la cui dimensione risulta essere:

$$\dim(V/W) = \dim(\text{span}([v_{k+1}], \dots, [v_n])) = n - k = \dim(V) - \dim(W)$$

□

8.3.1 Teorema del Rango

Proposizione 54: Nucleo ed Immagine di una trasformazione lineare

Data una trasformazione lineare $f : V \rightarrow W$, il nucleo $\ker(f) \subseteq V$ e l'immagine $\operatorname{im}(f) \subseteq W$ di f corrispondono a:

$$\ker(f) := \{v \in V \mid f(v) = 0_W\}$$

$$\operatorname{im}(f) := \{w \in W \mid f(v) = w, \exists v \in V\}$$

dove entrambi sono sottospazi vettoriali rispettivamente di V e W

Dimostrazione:

- Sappiamo già $\ker(f) \leq V$ e che $\operatorname{im}(f) \leq W$
- Verifichiamo quindi che siano chiusi nel prodotto per scalare

$$v \in \ker(f), \lambda \in K \implies f(\lambda v) = \lambda f(v) = \lambda 0_W = 0_W \implies \lambda v \in \ker(f)$$

$$w = f(v) \in \operatorname{im}(f), \lambda \in K \implies \lambda w = \lambda f(v) = f(\lambda v) \implies \lambda w \in \operatorname{im}(f)$$

□

Teorema 25: Primo teorema d'isomorfismo

Data una trasformazione lineare $f : V \rightarrow W$, si ha che

$$V/\ker(f) \cong \operatorname{im}(f)$$

(dimostrazione analoga agli altri casi del teorema)

Teorema 26: Teorema del Rango

Siano V e W due spazi vettoriali. Data una trasformazione lineare $f : V \rightarrow W$, definiamo come **rango di f** la dimensione della sua immagine, la quale equivale a:

$$\operatorname{rk}(f) := \dim(\operatorname{im}(f)) = \dim(V) - \dim(\ker(f))$$

Dimostrazione:

- Poiché $f : V \rightarrow W$ è una trasformazione lineare, per il primo teorema d'isomorfismo si ha che $V/\ker(f) \cong \operatorname{im}(f)$, da cui ne segue automaticamente che:

$$\begin{aligned} V/\ker(f) \cong \operatorname{im}(f) &\iff \dim(V/\ker(f)) = \dim(\operatorname{im}(f)) \iff \\ &\iff \dim(V) - \dim(\ker(f)) = \dim(\operatorname{im}(f)) \end{aligned}$$

□

8.4 Spazi affini, Sottospazi affini e Giacitura

Definizione 72: Spazio affine

Dato uno spazio vettoriale $(V, +, \cdot)$, definiamo come **spazio affine a V** la struttura (A, V, ϕ) , dove:

- Gli elementi $P \in A$ vengono detti **punti**
- La funzione $\phi : A \times V \rightarrow A$ gode delle seguenti proprietà

– **Associatività mista:**

$$\forall P \in A, \forall v, w \in V, \phi(\phi(P, v), w) = \phi(P, (v + w))$$

– **Elemento nullo destro:**

$$\forall a \in A, \exists 0_V \in V \mid \phi(a, 0_V) = a$$

– **Azione libera e transitiva:**

$$\forall P \in A, \text{ la funzione } \phi_P : V \rightarrow A : v \rightarrow \phi(P, v) \text{ è biettiva}$$

Detto in parole molto povere (e poco esatte) uno spazio affine A è una **traslazione totale di uno spazio vettoriale V** dove ogni punto del primo corrisponde biunivocamente ad un punto dell'altro

Definizione 73: Sottospazio affine e Giacitura

Dato uno spazio vettoriale V , un suo sottospazio vettoriale $W \subseteq V$ e un vettore $v \in V$, definiamo come **sottospazio affine** l'insieme di **punti** generato da:

$$U = v + W := \{v + w \mid w \in W\}$$

dove W viene definito **giacitura** di U , indicato con $\text{Giac}(U)$ e dove:

$$\dim(U) = \dim(\text{Giac}(U)) = \dim(W)$$

In altre parole, il sottospazio affine U corrisponde ad una **traslazione** del sottospazio W tramite il vettore v . Ogni sottospazio affine può essere visto come una **classe laterale di un sottospazio** (poiché l'operazione primaria è la somma).

8.5 Prodotto scalare e Spazio ortogonale

Definizione 74: Prodotto scalare

Dato lo spazio di coordinate K^n , definiamo come **prodotto scalare** l'operazione:

$$\cdot : K^n \times K^n \rightarrow K : ((\lambda_1, \dots, \lambda_n), (\mu_1, \dots, \mu_n)) \mapsto v \cdot v' = \sum_{i=1}^n \lambda_i \mu_i$$

la quale gode delle seguenti proprietà:

- $u, v \in K^n \implies u \cdot v = v \cdot u$ (**Simmetria**)
- $u, v, w \in K^n \implies (v + w)u = u(v + w) = vu + wu$ (**Distributività**)
- $u, v \in K^n, \lambda \in K \implies (\lambda u)v = u(\lambda v) = \lambda uv$ (**Linearità per scalare**)

Attenzione: il prodotto scalare differisce dal prodotto **per** scalare

Definizione 75: Norma di un vettore

Dato $v \in \mathbb{R}^n$, definiamo la **norma (o lunghezza)** di tale vettore come

$$\|v\| := \sqrt{v \cdot v} = \sqrt{x_1^2 + \dots + x_n^2}$$

Teorema 27

Dati $u, v \in \mathbb{R}^n$ e l'angolo $0 < \theta < \pi$ interno tra u e v , si ha che

$$\cos \theta = \frac{uv}{\|u\| \|v\|}$$

Inoltre, si verifica 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), si ha che:

$$\begin{aligned} \|v - u\|^2 &= \|u\|^2 + \|v\|^2 - 2 \|u\| \|v\| \cos \theta \iff \\ \iff \|v - u\|^2 - \|u\|^2 - \|v\|^2 &= -2 \|u\| \|v\| \cos \theta \iff \end{aligned}$$

$$\begin{aligned}
&\iff \sum_{i=1}^n (y_i - x_i)^2 - \sum_{j=1}^n x_j^2 - \sum_{k=1}^n y_k^2 = -2 \|u\| \|v\| \cos \theta \iff \\
&\iff \sum_{i=1}^n (y_i^2 - 2y_i x_i + x_i^2) - \sum_{j=1}^n x_j^2 - \sum_{k=1}^n y_k^2 = -2 \|u\| \|v\| \cos \theta \iff \\
&\iff \sum_{i=1}^n y_i^2 - 2 \sum_{h=1}^n y_h x_h + \sum_{t=1}^n x_t^2 - \sum_{j=1}^n x_j^2 - \sum_{k=1}^n y_k^2 = -2 \|u\| \|v\| \cos \theta \iff \\
&\iff \sum_{h=1}^n y_h x_h = \|u\| \|v\| \cos \theta \iff \sum_{h=1}^n y_h x_h = \|u\| \|v\| \cos \theta \iff \\
&\iff uv = \|u\| \|v\| \cos \theta \iff \frac{uv}{\|u\| \|v\|} = \cos \theta
\end{aligned}$$

□

Proposizione 55: Relazione di ortogonalità

Siano $u, v \in \mathbb{R}^n$. Il vettore u viene detto "**ortogonale a v** ", indicato come $v \perp w$, se e solo se:

$$u \perp v \iff uv = 0$$

Nota: l'ortogonalità è una generalizzazione del concetto di perpendicolarità nell'ambito dell'algebra lineare

Dimostrazione:

- Per definizione stessa di perpendicolarità, l'essere perpendicolari implica che vi sia un angolo retto tra due linee. Generalizzando tale concetto all'ortogonalità tra vettori, dato l'angolo $0 < \theta < \pi$ interno a u e v , per il teorema precedente si ha che:

$$uv = 0 \iff \theta = \frac{\pi}{2} \iff \cos(\theta) = 1 \iff \text{angolo retto tra } u \text{ e } v$$

□

Definizione 76: Sottospazio ortogonale

Dato il sottospazio vettoriale $V \subseteq K^n$, definiamo V^\perp il **sottospazio ortogonale a V** come:

$$V^\perp = \{v \in K^n \mid vw = 0, \forall w \in V\}$$

dove in particolare si ha che:

$$\dim(K^n) = \dim(V) + \dim(V^\perp)$$

Dimostrazione:

- $V^\perp \leq K^n$
 - $\forall v \in V, 0_{K^n} \cdot v = 0 \implies 0_{K^n} \in V^\perp$
 - $\forall v \in V, w_1, w_2 \in V^\perp \implies (w_1 + w_2)v = w_1v + w_2v = 0 + 0 = 0 \implies w_1 + w_2 \in V^\perp$
 - $\forall v \in V, w \in V^\perp \implies (-w)v = -(wv) = 0 \implies -w \in V^\perp$
- $\forall v \in V, w \in V^\perp, \lambda \in K \implies (\lambda w)v = \lambda(wv) = 0 \implies \lambda w \in V^\perp$
- Poiché $V \cap V^\perp = \{0_{K^n}\} \implies \dim(V \cap V^\perp) = 0$ e poiché $K^n = V + V^\perp$, per la formula di Grassman ne segue che:
$$\dim(K^n) = \dim(V + V^\perp) = \dim(V) + \dim(V^\perp) - \dim(V \cap V^\perp) = \dim(V) + \dim(V^\perp)$$

□

9

Matrici

Definizione 77: 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

$$A \in \text{Mat}_{m \times n}(K) \implies A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix}$$

dove $\text{Mat}_{m \times n}(K) = \underbrace{K^n \times \dots \times K^n}_{m \text{ volte}} = \underbrace{K^m \times \dots \times K^m}_{n \text{ volte}}$

Esempio:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \in \text{Mat}_{2 \times 3}(\mathbb{R})$$

Definizione 78: Vettori colonna e Vettori riga

Definiamo una matrice $1 \times n$ come **vettore riga**

$$\begin{pmatrix} a_1 & \cdots & a_n \end{pmatrix} \in \text{Mat}_{1 \times n}(K) = K^n$$

e analogamente definiamo una matrice $m \times 1$ come **vettore colonna**

$$\begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} \in \text{Mat}_{m \times 1}(K) = K^m$$

Osservazione 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)

$$A^1, \dots, A^m \in K^n \implies A = \begin{pmatrix} A^1 \\ \vdots \\ A^m \end{pmatrix}$$

Osservazione 56

La struttura $(\text{Mat}_{m \times n}(K), +, \cdot)$ è uno **spazio vettoriale** di dimensione:

$$\dim(\text{Mat}_{m \times n}(K)) = m \cdot n$$

e la cui **base canonica** è composta dalle matrici:

$$e_{i,j} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix} \left| \begin{cases} a_{k,h} = 0 & \text{se } k \neq i \vee h \neq j \\ a_{k,h} = 1 & \text{se } k = i, h = j \end{cases} \right.$$

Dimostrazione:

- Date $A, B \in \text{Mat}_{m \times n}(K)$ e $\lambda \in K$, le operazioni di somma e prodotto sono definite come:

$$A + B = \begin{pmatrix} a_{1,1} + b_{1,1} & \cdots & a_{1,n} + b_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} + b_{m,1} & \cdots & a_{m,n} + b_{m,n} \end{pmatrix}$$

$$\lambda A = \begin{pmatrix} \lambda a_{1,1} & \cdots & \lambda a_{1,n} \\ \vdots & \ddots & \vdots \\ \lambda a_{m,1} & \cdots & \lambda a_{m,n} \end{pmatrix}$$

- Le dimostrazioni di $(\text{Mat}_{m \times n}(K), +, \cdot)$ spazio vettoriale e della base canonica vengono omesse poiché analoghe alle dimostrazioni per K^n

□

Esempio:

- La base canonica di $\text{Mat}_{2 \times 2}(A)$ corrisponde a:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Osservazione 57

Dato lo spazio $\text{Mat}_{m \times n}(K)$, si ha che:

$$\text{Mat}_{m \times n}(K) \cong K^{m \cdot n}$$

Dimostrazione:

- Poiché $\dim(\text{Mat}_{m \times n}(K)) = m \cdot n$ e $\dim(K^{m \cdot n}) = m \cdot n$, per dimostrazione precedente si ha che:

$$\dim(\text{Mat}_{m \times n}(K)) = \dim(K^{m \cdot n}) \iff \text{Mat}_{m \times n}(K) \cong K^{m \cdot n}$$

□

Definizione 79: Prodotto tra matrici

Sia $A = (A_1, \dots, A_h) \in \text{Mat}_{h \times m}(K)$ e sia $B = (B^1, \dots, B^n) \in \text{Mat}_{m \times n}(K)$.

Definiamo come **prodotto tra matrici** la trasformazione lineare:

$$\cdot : \text{Mat}_{h \times m}(K) \times \text{Mat}_{m \times n}(K) \rightarrow \text{Mat}_{h \times n}(K) : (A, B) \mapsto AB$$

dove :

$$AB = \begin{pmatrix} A_1 B^1 & \dots & A_1 B^n \\ \vdots & \ddots & \vdots \\ A_h B^1 & \dots & A_h B^n \end{pmatrix}$$

Attenzione: affinché il prodotto sia 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

Osservazione 58

Date tre matrici A, B, C ed uno scalare λ , se i prodotti sono **ben definiti** si ha che:

- $(AB)C = ABC = A(BC)$
- $A(B + C) = AB + AC$
- $(A + B)C = AC + BC$
- $\lambda(AB) = (\lambda A)B = A(\lambda B)$

Corollario 25

Uno spazio vettoriale $\text{Mat}_{n \times n}(K)$ (anche detto spazio delle matrici quadrate di ordine n) è un **anello non commutativo**, dove l'elemento neutro è:

$$I_n = \begin{pmatrix} 1 & 0 & \dots & \dots & 0 \\ 0 & 1 & 0 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & 0 & 1 & 0 \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix}$$

9.1 Rango di una matrice

Definizione 80: Trasformazione lineare di una matrice

Data una matrice $A \in \text{Mat}_{m \times n}(K)$, definiamo la **trasformazione lineare associata ad A** come

$$L_A : K^n \rightarrow K^m : x := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \rightarrow Ax$$

dove:

$$L_A(x) = Ax = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{1,1}x_1 + \cdots + a_{1,n}x_n \\ \vdots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n \end{pmatrix}$$

Definizione 81: Sistema lineare e Matrice completa

Data una **matrice di coefficienti** A ed un **vettore di incognite** b , definiti come:

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix} \quad b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

l'equazione $Ax = b$ corrisponde ad un **sistema lineare di equazioni cartesiane** nella forma:

$$\begin{cases} a_{1,1}x_1 + \cdots + a_{1,n}x_n = b_1 \\ \vdots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n = b_m \end{cases}$$

il quale è rappresentato fedelmente dalla seguente **matrice completa**:

$$A_b = \left(\begin{array}{ccc|c} a_{1,1} & \cdots & a_{1,n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m,1} & \cdots & a_{m,n} & b_m \end{array} \right)$$

Dimostrazione:

- Si nota facilmente che:

$$\begin{aligned} Ax = b &\iff \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \iff \\ &\iff \begin{pmatrix} a_{1,1}x_1 + \cdots + a_{1,n}x_n \\ \vdots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \iff \begin{cases} a_{1,1}x_1 + \cdots + a_{1,n}x_n = b_1 \\ \vdots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n = b_n \end{cases} \end{aligned}$$

□

Proposizione 56

Data una matrice $A \in \text{Mat}_{m \times n}(K)$, si ha che:

- $\text{im}(L_A) = \text{span}(A^1, \dots, A^n)$
- $\ker(L_A) = \text{span}(A_1, \dots, A_m)^\perp$

Dimostrazione:

- Data $A \in \text{Mat}_{m \times n}(K)$, si ha che:

$$\begin{aligned} L_A(x) \in \text{im}(L_A) &\iff L_A(x) = Ax = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \\ &x_1 \begin{pmatrix} a_{1,1} \\ \vdots \\ a_{m,1} \end{pmatrix} + \cdots + x_n \begin{pmatrix} a_{1,n} \\ \vdots \\ a_{m,n} \end{pmatrix} = x_1 A^1 + \cdots + x_n A^n \iff L_A(x) \in \text{span}(A^1, \dots, A^n) \end{aligned}$$

dunque si ha che $\text{im}(L_A) = \text{span}(A^1, \dots, A^n)$

- Inoltre, notiamo che:

$$\begin{aligned} \ker(L_A) &= \{x \in K^n \mid L_A(x) = Ax = 0_{K^m}\} = \\ &= \left\{ x \in K^n \mid \begin{pmatrix} A_1 \\ \vdots \\ A_m \end{pmatrix} x = 0_{K^m} \right\} = \text{span}(A_1, \dots, A_m)^\perp \end{aligned}$$

dunque $\ker(L_A)$ contiene tutte i vettori $x = (x_1, \dots, x_n) \in K^n$ che sono soluzione del seguente sistema:

$$\begin{cases} a_{1,1}x_1 + \cdots + a_{1,n}x_n = 0 \\ \vdots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n = 0 \end{cases}$$

□

Definizione 82: Rango di una matrice

Data una matrice $A \in \text{Mat}_{m \times n}(K)$, definiamo come **rango di A** il rango della sua trasformazione lineare associata:

$$\text{rk}(A) := \text{rk}(L_A)$$

Proposizione 57

Data una matrice $A \in \text{Mat}_{m \times n}(K)$, si ha che:

$$\text{rk}(A) = n - \dim(\ker(L_A)) = \dim(\text{span}(A^1, \dots, A^n)) = \dim(\text{span}(A_1, \dots, A_m))$$

Dimostrazione:

- Poiché $\text{rk}(A) := \text{rk}(L_A)$ e poiché $L_A : K^n \rightarrow K^m$, per il teorema del rango si ha che:

$$\text{rk}(A) := \text{rk}(L_A) = \dim(L_A) = \dim(K^n) - \dim(\ker(L_A)) = n - \dim(\ker(L_A))$$

- Inoltre, per dimostrazioni precedenti si ha che:

$$\begin{aligned} \dim(\text{span}(A^1, \dots, A^n)) &= \dim(\text{im}(L_A)) = n - \dim(\ker(L_A)) = \\ &= n - \dim(\text{span}(A_1, \dots, A_m)^\perp) = \dim(\text{span}(A_1, \dots, A_m)) \end{aligned}$$

□

Corollario 26

Data una matrice $A \in \text{Mat}_{m \times n}(K)$, si ha che:

$$0 \leq \text{rk}(A) \leq \min(m, n)$$

9.1.1 Riduzione a scala di una matrice**Definizione 83: Operazioni elementari su matrici**

Data una matrice $A \in \text{Mat}_{m \times n}(K)$, definiamo come **operazioni elementari** su righe e colonne le seguenti tre operazioni:

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)

Definizione 84: Matrici equivalenti

Date due matrici $A, B \in \text{Mat}_{m \times n}(K)$, definiamo tali matrici come **equivalenti** se sono uguali se è possibile ottenere l'una partendo dall'altra utilizzando **solo operazioni elementari**.

In particolare, se vengono utilizzate solo operazioni su righe tali matrici vengono dette **equivalenti per righe**, mentre vengono dette **equivalenti per colonne** se vengono utilizzate solo operazioni su colonne.

Osservazione 59

Date due matrici $A, B \in \text{Mat}_{m \times n}(K)$, si ha che:

- Se A e B sono **equivalenti per righe**, allora

$$\ker(L_A) = \ker(L_B) \wedge \text{im}(L_A) \neq \text{im}(L_B)$$

- Se A e B sono **equivalenti per colonne**, allora

$$\ker(L_A) \neq \ker(L_B) \wedge \text{im}(L_A) = \text{im}(L_B)$$

In entrambi i casi si verifica che:

$$\text{rk}(A) = \text{rk}(B)$$

Dimostrazione:

- Basti pensare che effettuando solo operazioni su righe non si vadano ad alterare i vettori $x \in \ker(L_A)$ in grado di risolvere il sistema $Ax = 0$, dunque $\ker(L_A) = \ker(L_B)$, mentre i vettori $b \in \text{im}(L_A)$ generati dal sistema $Ax = b$ vanno ad essere modificati, dunque $\text{im}(L_A) \neq \text{im}(L_B)$
- Analogamente, effettuando solo operazioni su colonne non si vanno ad alterare i vettori $b \in \text{im}(L_A)$ generati dal sistema $Ax = b$, dunque $\text{im}(L_A) = \text{im}(L_B)$, mentre i vettori $x \in \ker(L_A)$ risolvono il sistema $Ax = b$ vanno ad essere modificati, dunque $\ker(L_A) \neq \ker(L_B)$
- Nel caso in cui il nucleo non venga alterato, si ha che:

$$\begin{aligned} \text{rk}(A) &= \dim(\text{im}(L_A)) = n - \dim(\ker(L_A)) = \\ &= n - \dim(\ker(L_B)) = \dim(\text{im}(L_B)) = \text{rk}(B) \end{aligned}$$

mentre nel caso in cui l'immagine non venga alterata si ha che:

$$\text{rk}(A) = \dim(\text{im}(L_A)) = \dim(\text{im}(L_B)) = \text{rk}(L_B)$$

□

Definizione 85: Pivot e Matrice a scala

Data una matrice $A \in \text{Mat}_{m \times n}(K)$, definiamo come **pivot** di una riga il primo elemento non nullo a partire da sinistra di tale riga.

Inoltre, la matrice A 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:

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 3 & 3 \\ 0 & 9 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 6 \\ 0 & 0 & 3 \\ 8 & 0 & 0 \end{pmatrix}$$

Algoritmo 1: 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

Teorema 28: Riduzione a scala

Sia $A = (A^1, \dots, A^n) \in \text{Mat}_{m \times n}(K)$ e sia $S = (S^1, \dots, S^n)$ la sua versione ridotta a scala.

Se S^{j_1}, \dots, S^{j_h} sono le colonne di S contenenti i pivot della scala, allora A^{j_1}, \dots, A^{j_h} sono una base di $\text{im}(A) = \text{span}(A^1, \dots, A^n)$, implicando che

$$h = \text{rk}(S) = \text{rk}(A)$$

Esempio:

- Consideriamo il seguente sistema e la matrice completa ad essa associata:

$$\begin{cases} x + 2y + 3z = 0 \\ 4x + 5y + 6z = 0 \\ 7x + 8y + 9z = 0 \end{cases} \implies A_b = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

dove il vettore incognito b viene omissso dalla matrice completa in quanto $b = 0_{K^m}$

- Date le righe R_1, \dots, R_3 della matrice, procediamo quindi con l'algoritmo di Gauss-Jordan fino ad ottenere la versione a scala di tale matrice:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \xrightarrow{R_2-4R_1, R_3-7R_1} \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{pmatrix} \xrightarrow{R_3-2R_2} \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix}$$

- Dunque, otteniamo che A^1 e A^2 sono una base di $\text{im}(L_A) = \text{span}(A^1, A^2, A^3)$ e il rango della matrice corrisponde a $\text{rk}(A) = 2$
- Riducendo ancora tale matrice (mantenendo la forma a scala), si ha che:

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{-\frac{1}{3}R_2} \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{R_1-2R_2} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

- Dunque, il sistema di partenza risulta essere equivalente al seguente:

$$\begin{cases} x + 2y + 3z = 0 \\ 4x + 5y + 6z = 0 \\ 7x + 8y + 9z = 0 \end{cases} \iff \begin{cases} x - z = 0 \\ y + 2z = 0 \end{cases}$$

- Poiché abbiamo svolto solo operazioni per riga, la matrice originale e la sua versione a scala risultano essere equivalenti per righe, implicando che il nucleo non sia stato alterato.
- Di conseguenza, risolvendo tale sistema in funzione di una variabile ausiliaria t , siamo in grado di ottenere una base di $\ker(L_A)$:

$$\begin{cases} x - z = 0 \\ y + 2z = 0 \end{cases} \implies \begin{cases} x = z \\ y = -2z \end{cases} \implies \begin{cases} x = t \\ y = -2t \\ z = t \end{cases} \implies \begin{pmatrix} x \\ y \\ z \end{pmatrix} = t \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}$$

- Infine, quindi, concludiamo che:

$$\begin{pmatrix} 1 \\ 4 \\ 7 \end{pmatrix}, \begin{pmatrix} 2 \\ 5 \\ 8 \end{pmatrix} \text{ base di } \text{im}(L_A) \qquad \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} \text{ base di } \ker(L_A)$$

9.2 Teorema di Rouché-Capelli

Teorema 29: 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.

$$\exists x \in K^n \mid Ax = b \iff \text{rk}(A) = \text{rk}(A_b)$$

Dimostrazione:

- Dato il sistema $Ax = b$, si verifica che:

$$\begin{aligned} \exists x \in K^n \mid Ax = b &\iff \exists x_1, \dots, x_n \in K \mid x_1 A^1 + \dots + x_n A^n = b \iff \\ &\iff b \in \text{span}(A^1, \dots, A^n) \iff \text{span}(A^1, \dots, A^n) = \text{span}(A^1, \dots, A^n, b) \iff \\ &\iff \dim(\text{span}(A^1, \dots, A^n)) = \dim(\text{span}(A^1, \dots, A^n, b)) \iff \text{rk}(A) = \text{rk}(A_b) \end{aligned}$$

□

Proposizione 58

Dato il sistema $Ax = b$, l'insieme delle soluzioni V (se esistenti) è un **sottospazio affine** di $\ker(L_A)$ di dimensione $\dim(V) = n - \text{rk}(A)$, dove in particolare si ha che:

- Se $\text{rk}(A) = \text{rk}(A_b) = n$, la soluzione al sistema è **unica** e il sistema viene detto **determinato**

$$\exists! x \in K^n \mid Ax = b \iff \text{rk}(A) = \text{rk}(A_b) = n$$

- Se $\text{rk}(A) = \text{rk}(A_b) \neq n$, allora il sistema ammette **infinite soluzioni** e il sistema viene detto **indeterminato**

$$\exists x \in K^n \mid Ax = b \iff \text{rk}(A) = \text{rk}(A_b) \neq n$$

Dimostrazione:

- Dato $V = \{x \in K^n \mid Ax = b\}$ l'insieme delle soluzioni del sistema (ipotizzando che ne esista almeno una), si ha che:

$$x_0, x \in V \iff Ax_0 = b = Ax \iff Ax_0 = Ax \iff A(x - x_0) = 0$$

$$\iff x' - x_0 \in \ker(L_A) \iff x' \in x_0 + \ker(L_A)$$

dunque V è un sottospazio affine a $\ker(L_A)$ traslato da una soluzione particolare x_0 del sistema

- In quanto sottospazio affine del nucleo, ne segue che:

$$\begin{aligned}\dim(V) &= \dim(\ker(L_A)) = \dim(K^n) - \dim(\operatorname{im}(L_A)) = n - \dim(\operatorname{im}(L_A)) \\ &= n - \operatorname{rk}(A) = \begin{cases} 0 & \text{se } \operatorname{rk}(A) = n \\ > 1 & \text{se } \operatorname{rk}(A) \neq n \end{cases}\end{aligned}$$

- Dunque, nel caso in cui $\operatorname{rk}(A) = n$ l'unica soluzione all'interno di V sarà x_0 , altrimenti esisteranno infinite soluzioni generate dalla traslazione della base di $\ker(L_A)$

□

Esempi:

1. • Consideriamo il seguente sistema lineare:

$$\begin{aligned}\begin{cases} w + 2x + z = 1 \\ 2w + 4x + y = 3 \\ w + 2x + y - z = 2 \end{cases} &\implies A_b = \left(\begin{array}{cccc|c} 1 & 2 & 0 & 1 & 1 \\ 2 & 4 & 1 & 0 & 3 \\ 1 & 2 & 1 & -1 & 2 \end{array} \right) \xrightarrow{R_3 - R_1, R_2 - 2R_1} \\ &\xrightarrow{R_3 - R_1, R_2 - 2R_1} \left(\begin{array}{cccc|c} 1 & 2 & 0 & 1 & 1 \\ 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & 1 & -2 & 1 \end{array} \right) \xrightarrow{R_3 - R_2} \left(\begin{array}{cccc|c} 1 & 2 & 0 & 1 & 1 \\ 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)\end{aligned}$$

- Dunque, poiché $\operatorname{rk}(A) = \operatorname{rk}(A_b) = 2 \neq 4$, il sistema ammette infinite soluzioni e le colonne A^1, A^3 sono base di $\operatorname{im}(L_A)$. Inoltre, il sistema è equivalente a:

$$\begin{aligned}\begin{cases} w + 2x + z = 1 \\ y - 2z = 1 \end{cases} &\iff \begin{cases} w = 1 - 2x - z \\ y = 1 + 2z \end{cases} \iff \\ \iff \begin{cases} w = 1 - 2t_1 - t_2 \\ x = t_1 \\ y = 1 + 2t_2 \\ z = t_1 \end{cases} &\iff \begin{pmatrix} w \\ x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + t_1 \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \end{pmatrix} + t_2 \begin{pmatrix} -1 \\ 0 \\ 2 \\ 1 \end{pmatrix}\end{aligned}$$

2. • Consideriamo il seguente sistema

$$\begin{aligned}\begin{cases} x + y + z = 1 \\ -x + y + 5z = 0 \\ 2y + 6z = 0 \end{cases} &\implies A_b = \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ -1 & 1 & 5 & 0 \\ 0 & 2 & 6 & 0 \end{array} \right) \xrightarrow{R_2 + R_1} \\ &\xrightarrow{R_2 + R_1} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 2 & 6 & 1 \\ 0 & 2 & 6 & 0 \end{array} \right) \xrightarrow{R_3 - R_2} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 2 & 6 & 1 \\ 0 & 0 & 0 & -1 \end{array} \right)\end{aligned}$$

- Poiché $\operatorname{rk}(A) \neq \operatorname{rk}(A_b)$, il sistema non ammette soluzioni

3. • Consideriamo il seguente sistema:

$$\begin{cases} x + ky = 4 - k \\ kx + 4y = 4 \end{cases} \implies A_b = \left(\begin{array}{cc|c} 1 & k & 4 - k \\ k & 4 & 4 \end{array} \right) \xrightarrow{R_2 - kR_1} \xrightarrow{R_2 - kR_1} \left(\begin{array}{cc|c} 1 & k & 4 - k \\ 0 & 4 - k^2 & 4 - 2k + k^2 \end{array} \right) = \left(\begin{array}{cc|c} 1 & k & 4 - k \\ 0 & 4 - k^2 & (2 - k)^2 \end{array} \right)$$

- A questo punto, a seconda del valore di k si verificano tre casi:
 - Se $k \neq \pm 2$, ne segue che $4 - k^2 \neq 0$ e di conseguenza che $\text{rk}(A) = \text{rk}(A_b) = 2$, implicando che il sistema ammetta un'unica soluzione
 - Se $k = -2$, si ha che $\text{rk}(A) \neq \text{rk}(A_b)$, dunque il sistema non ammette soluzioni
 - Se $k = 2$, si ha che $\text{rk}(A) = \text{rk}(A_b) = 1 \neq 2$, dunque il sistema ammette infinite soluzioni

$$A_b = \left(\begin{array}{cc|c} 1 & 2 & 2 \\ 0 & 0 & 0 \end{array} \right) \iff \{x + 2y = 2\} \implies \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \end{pmatrix} + t \begin{pmatrix} -2 \\ 2 \end{pmatrix}$$

9.2.1 Equazioni parametriche

Proposizione 59: Equazioni parametriche

Sia V un sottospazio e sia W un sottospazio affine al un sottospazio $\text{Giac}(W) \subseteq V$, dunque $\exists x_0 \in V \mid W = x_0 + \text{Giac}(W)$.

Data la base g_1, \dots, g_n di $\text{Giac}(W)$, si verifica che:

$$\forall x \in W, \exists! t_1, \dots, t_n \in K \mid x = x_0 + t_1 g_1 + \dots + t_n g_n$$

Definiamo l'insieme di tali equazioni come **equazioni parametriche** di W

Dimostrazione:

- Dato $x_0 \in V \mid W = x_0 + \text{Giac}(W)$ e data la base g_1, \dots, g_n di $\text{Giac}(W)$, si ha che:

$$\begin{aligned} x \in W &\iff x - x_0 \in \text{Giac}(W) \iff \\ &\iff \exists! t_1, \dots, t_n \in K \mid x - x_0 = t_1 g_1 + \dots + t_n g_n \\ &\iff x = x_0 + t_1 g_1 + \dots + t_n g_n \end{aligned}$$

□

Proposizione 60

Dato uno spazio vettoriale V e un sottospazio affine W espresso come l'insieme delle sue equazioni parametriche:

$$W = \{x_0 + t_1 g_1 + \dots + t_n g_n \mid t_1, \dots, t_n \in K\}$$

dove g_1, \dots, g_n sono base di $\text{Giac}(W)$, si verifica che:

$$x \in W \iff \text{rk}(A_b) = \dim(V)$$

dove $A_b := (g_1, \dots, g_n, x - x_0) \in \text{Mat}_{n \times n}(K)$

Dimostrazione:

- Data la matrice $A_b := (g_1, \dots, g_n, x - x_0)$, per il teorema di Rouché-Capelli, si ha che:

$$\begin{aligned} x \in W &\iff x - x_0 \in \text{Giac}(W) = \text{span}(g_1, \dots, g_n) \iff \\ &\iff \text{span}(g_1, \dots, g_n) = \text{span}(g_1, \dots, g_n, x - x_0) \iff \\ &\iff \dim(\text{span}(g_1, \dots, g_n)) = \dim(\text{span}(g_1, \dots, g_n, x - x_0)) \iff \\ &\iff \dim(\text{Giac}(W)) = \text{rk}(A_b) \iff \dim(W) = \text{rk}(A_b) \end{aligned}$$

□

Esempio:

- Consideriamo il seguente insieme di equazioni parametriche corrispondenti ad un sottospazio affine in \mathbb{R}^3

$$V = \left\{ \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} + t_1 \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + t_2 \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} \mid t_1, t_2 \in \mathbb{R} \right\}$$

- Poiché $\dim(V) = 2$, 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:

$$\begin{cases} x - 2y + z = 0 \end{cases}$$

corrispondente ad una retta in \mathbb{R}^3

9.3 Determinante di una matrice

Definizione 86: 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:

$$f(v_1, \dots, \lambda v'_i + \mu v''_i, \dots, v_n) = \lambda f(v_1, \dots, v'_i, \dots, v_n) + \mu f(v_1, \dots, v''_i, \dots, v_n)$$

Definizione 87: Determinante di una matrice

Definiamo come **determinante** di una matrice l'unica trasformazione lineare

$$\det : \text{Mat}_{n \times n}(K) \rightarrow K$$

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 **basi** di K^n se e solo se $\det(A) \neq 0$
3. $\det(I_n) = 1$, dove I_n è la matrice identità di ordine n

Osservazione 60

Data una matrice $A \in M_{n \times n}(K)$, si ha che:

- $\exists A_i, A_j \in A, i \neq j \mid A_i = A_j \implies \det(A) = 0$
- $\exists A^i, A^j \in A, i \neq j \mid A^i = A^j \implies \det(A) = 0$
- $\exists A_i \in A \mid A_i = 0_{K^n} \implies \det(A) = 0$
- $\exists A^i \in A \mid A^i = 0_{K^n} \implies \det(A) = 0$

Dimostrazione:

- Se esistono due righe $A_i, A_j \in A$ uguali, allora $\text{span}(A_1, \dots, A_n)$ non è linearmente indipendente, dunque non può costituire base di K^n
- Se esiste una riga $A_h \in A$ uguale al vettore nullo, allora $\text{span}(A_1, \dots, A_n)$ non è né linearmente indipendente né generatore di K^n , dunque non può costituire base di K^n
- Per le colonne vale il ragionamento analogo alle righe

□

Proposizione 61: Determinante alternante su righe e colonne

Data una matrice $A = (A_1, \dots, A_i, \dots, A_j, \dots, A_n) \in \text{Mat}_{n \times n}(K)$, 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:

- 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:

$$\begin{aligned} 0 &= \det(A_1, \dots, A_i + A_j, \dots, A_i + A_j, \dots, A_n) \implies \\ \implies 0 &= \det(A_1, \dots, A_i, \dots, A_i + A_j, \dots, A_n) + \det(A_1, \dots, A_j, \dots, A_i + A_j, \dots, A_n) \implies \\ \implies 0 &= \det(A_1, \dots, A_i, \dots, A_i, \dots, A_n) + \det(A_1, \dots, A_i, \dots, A_j, \dots, A_n) + \\ &\quad + \det(A_1, \dots, A_j, \dots, A_i, \dots, A_n) + \det(A_1, \dots, A_j, \dots, A_j, \dots, A_n) \implies \\ \implies 0 &= 0 + \det(A_1, \dots, A_i, \dots, A_j, \dots, A_n) + \det(A_1, \dots, A_j, \dots, A_i, \dots, A_n) + 0 \implies \\ \implies \det(A_1, \dots, A_i, \dots, A_j, \dots, A_n) &= -\det(A_1, \dots, A_j, \dots, A_i, \dots, A_n) \end{aligned}$$

□

Teorema 30: Teorema di Binet

Date due matrici $A, B \in \text{Mat}_{n \times n}(K)$, si ha che:

$$\det(AB) = \det(A) \cdot \det(B)$$

(dimostrazione omessa)

9.3.1 Formula di Leibniz e Regola di Sarrus

Definizione 88: Formula di Leibniz

Tramite le sue proprietà 1), 3) e la sua alternanza su righe e colonne, il determinante di una matrice $A \in \text{Mat}_{n \times n}(K)$ può essere definito come:

$$\det(A) := \sum_{\sigma \in S_n} \text{sgn}(\sigma) \cdot a_{1,\sigma(1)} \cdot \dots \cdot a_{n,\sigma(n)}$$

(dimostrazione omessa)

Corollario 27

Se $A \in \text{Mat}_{2 \times 2}(K)$, 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:

$$\det(A) = \sum_{\sigma \in S_2} \text{sgn}(\sigma) \cdot a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} = a_{1,1}a_{2,2} - a_{1,2}a_{2,1} = ad - bc$$

□

Corollario 28

Se $A \in \text{Mat}_{3 \times 3}(K)$, 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

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} := \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

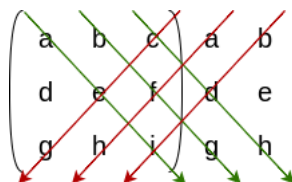
- Dato $S_3 = \{(1)(2)(3), (12)(3), (1)(23), (13)(2), (123), (321)\}$, si verifica che:

$$\begin{aligned}\det(A) &= \sum_{\sigma \in S_3} \operatorname{sgn}(\sigma) \cdot a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdot a_{3,\sigma(3)} = \\ &= a_{1,1}a_{2,2}a_{3,3} - a_{1,2}a_{2,1}a_{3,3} - a_{1,1}a_{2,3}a_{3,2} - a_{1,3}a_{2,2} - a_{3,1} + a_{1,2}a_{2,3}a_{3,1} + a_{1,3}a_{2,1}a_{3,2} = \\ &= aei - bdi - ceg - afh + bfg + cdh\end{aligned}$$

□

Metodo 3: Regola di Sarrus

La **Regola di Sarrus** permette di 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 diagonali** e **sottrarre le tre anti-diagonali**:



$$A \in \operatorname{Mat}_{3 \times 3}(K) \implies \det(A) = aei + bfg + cdh - afh - dfi - ceg$$

Esempi:

- 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

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 0 \end{pmatrix}$$

si ha che:

$$\det(A) = 1 \cdot 5 \cdot 0 + 2 \cdot 6 \cdot 7 + 3 \cdot 4 \cdot 8 - 2 \cdot 4 \cdot 0 - 3 \cdot 5 \cdot 7 - 1 \cdot 6 \cdot 8 = 27$$

9.3.2 Determinante tramite riduzione a scala

Definizione 89: Matrice triangolare

Sia $A \in \text{Mat}_{n \times n}(K)$. Definiamo A come **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

$$A = \begin{pmatrix} a_{1,1} & 0 & \cdots & \cdots & 0 \\ a_{1,2} & a_{2,2} & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & a_{n-1,n-2} & a_{n-1,n-1} & 0 \\ a_{n,1} & \cdots & \cdots & a_{n,n-1} & a_{n,n} \end{pmatrix}$$

Osservazione 61

Una **matrice a scala** è sempre **triangolare**.

Osservazione 62

Se $A \in \text{Mat}_{n \times n}(K)$ è una matrice triangolare, allora il suo determinante corrisponde al **prodotto della sua diagonale**

$$\det(A) = a_{1,1} \cdot a_{2,2} \cdot \dots \cdot a_{n,n}$$

(dimostrazione omessa)

Metodo 4: Calcolo del determinante tramite riduzione a scala

Data una matrice $A \in \text{Mat}_{n \times n}(K)$, 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 della matrice 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:

- Sia $A = (A_1, \dots, A_i, \dots, A_j, \dots, A_n) \in \text{Mat}_{n \times n}(K)$
- 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 $A' = (A_1, \dots, \lambda A_i, \dots, A_j, \dots, A_n) \in \text{Mat}_{n \times n}(K)$, per multilinearità del determinante si ha che:

$$\begin{aligned} \det(A') &= \det(A_1, \dots, \lambda A_i, \dots, A_j, \dots, A_n) = \\ &= \lambda \cdot \det(A_1, \dots, A_i, \dots, A_j, \dots, A_n) = \lambda \det(A) \end{aligned}$$

- Data $A'' = (A_1, \dots, A_i + \mu A_j, \dots, A_j, \dots, A_n) \in \text{Mat}_{n \times n}(K)$, 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:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 0 \end{pmatrix}$$

- Effettuiamo la riduzione a scala di tale matrice:

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 0 \end{pmatrix} &\xrightarrow{R_2-4R_1} \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 7 & 8 & 0 \end{pmatrix} \xrightarrow{R_3-7R_1} \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -21 \end{pmatrix} \\ &\xrightarrow{R_2 \cdot \frac{1}{3}} \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & -6 & -21 \end{pmatrix} \xrightarrow{R_3+6R_2} \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & -9 \end{pmatrix} \end{aligned}$$

- Poiché una matrice a scala è sempre triangolare, si ha che:

$$S := \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & -9 \end{pmatrix} \implies \det(S) = 1 \cdot 1 \cdot (-9) = -9$$

- Tra i vari passaggi effettuati durante la riduzione a scala, l'unico ad influenzare il determinante è il terzo. Dunque, si ha che:

$$\det(S) = -\frac{1}{3} \cdot \det(A) \implies -9 = -\frac{1}{3} \cdot \det(A) \implies \det(A) = 27$$

9.3.3 Sviluppo di Laplace

Definizione 90: 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

Definizione 91: Minore di una matrice

Data una matrice $A \in \text{Mat}_{m \times n}(K)$, 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 .

Teorema 31: Sviluppo di Laplace

Data una matrice $A \in \text{Mat}_{n \times n}(K)$, 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:

$$\det(A) = \sum_{h=1}^n (-1)^{h+j} \cdot a_{h,j} \cdot \det(M_{h,j}) = \sum_{h=1}^n a_{h,j} \cdot \text{cof}_{h,j}(A)$$

(dimostrazione omessa)

Esempi:

1. • Riprendiamo la matrice già vista in vari esempi precedenti, il cui determinante sappiamo già essere 27:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 0 \end{pmatrix}$$

- Effettuiamo lo sviluppo di Laplace su A_3 :

$$\begin{aligned} \det(A) &= (-1)^{3+1} \cdot 7 \cdot \det \begin{pmatrix} 2 & 3 \\ 5 & 6 \end{pmatrix} + (-1)^{3+2} \cdot 8 \cdot \det \begin{pmatrix} 1 & 3 \\ 4 & 6 \end{pmatrix} + (-1)^{3+3} \cdot 0 \cdot \det \begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix} = \\ &= 7(2 \cdot 6 - 3 \cdot 5) - 8(1 \cdot 6 - 3 \cdot 4) + 0 = -21 + 48 = 27 \end{aligned}$$

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:

$$\begin{aligned} \det(A) &= -5 \cdot \det \begin{pmatrix} 1 & 4 & -1 \\ 7 & 8 & -2 \\ 0 & 1 & 6 \end{pmatrix} = -5 \left[(-1)^{1+1} \cdot 1 \cdot \det \begin{pmatrix} 8 & -2 \\ 1 & 6 \end{pmatrix} + \right. \\ &\quad \left. + (-1)^{2+1} \cdot 7 \cdot \det \begin{pmatrix} 4 & -1 \\ 1 & 6 \end{pmatrix} \right] = -5[50 - 175] = 625 \end{aligned}$$

9.3.4 Regola di Cramer

Teorema 32: 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:

$$\begin{cases} x_1 = \frac{1}{\det(A)} \cdot \det(b, A^2, \dots, A^{n-1}, A^n) \\ x_2 = \frac{1}{\det(A)} \cdot \det(A^1, b, \dots, A^{n-1}, A^n) \\ \vdots \\ x_{n-1} = \frac{1}{\det(A)} \cdot \det(A^1, A^2, \dots, b, A^n) \\ x_n = \frac{1}{\det(A)} \cdot \det(A^1, A^2, \dots, A^{n-1}, b) \end{cases}$$

(dimostrazione omessa)

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:

$$\begin{cases} x = \frac{1}{27} \cdot \det \begin{pmatrix} 1 & 2 & 3 \\ 0 & 5 & 6 \\ 0 & 8 & 0 \end{pmatrix} \\ y = \frac{1}{27} \cdot \det \begin{pmatrix} 1 & 1 & 3 \\ 4 & 0 & 6 \\ 7 & 0 & 0 \end{pmatrix} \\ z = \frac{1}{27} \cdot \det \begin{pmatrix} 1 & 2 & 1 \\ 4 & 5 & 0 \\ 7 & 8 & 0 \end{pmatrix} \end{cases} \iff \begin{cases} x = \frac{1}{27} \cdot (-48) \\ y = \frac{1}{27} \cdot (42) \\ z = \frac{1}{27} \cdot (-3) \end{cases} \iff \begin{cases} x = -\frac{16}{9} \\ y = \frac{14}{9} \\ z = -\frac{1}{9} \end{cases}$$

9.4 Matrici inverse

Definizione 92: Gruppo generale lineare

Definiamo come **gruppo generale lineare** il gruppo $(GL(n, K), \cdot)$ contenente tutte le matrici invertibili dell'anello $\text{Mat}_{n \times n}(K)$:

$$GL(n, K) = \{A \in \text{Mat}_{n \times n}(K) \mid \exists A^{-1} \in \text{Mat}_{n \times n}(K)\}$$

Dimostrazione:

- $A, B, C \in GL(n, K), A(BC) = ABC = (AB)C$
- $\forall A \in GL(n, K), \exists I_n \in GL(n, K) \mid AI_n = I_n A = A$

- $\forall A \in GL(n, K), \exists! A^{-1} \in GL(n, K) \mid AA^{-1} = A^{-1}A = I_n$

□

Teorema 33: Invertibilità di una matrice

Data una matrice $A \in \text{Mat}_{n \times n}(K)$, le seguenti condizioni sono equivalenti tra loro:

1. $A \in GL(n, K)$
2. $\text{rk}(A) = n$
3. $\det(A) \neq 0$
4. A^1, \dots, A^n sono una base di K^n
5. A^1, \dots, A^n sono una base di K^n
6. A è equivalente per righe e colonne a I_n

Dimostrazione:

- 3) \iff 4), 5)

– Per definizione stessa di determinante, si ha che:

$$\det(A) \neq 0 \iff \begin{cases} A^1, \dots, A^n \text{ base di } K^n \\ A_1, \dots, A_n \text{ base di } K^n \end{cases}$$

- 2) \iff 3), 4)

– Poiché $\dim(K^n) = n$ implica che n vettori possono essere generatori se e solo se sono anche linearmente indipendenti, si ha che:

$$\text{rk}(A) = n \iff \dim(\text{span}(A^1, \dots, A^n)) = \dim(\text{span}(A_1, \dots, A_n)) = n \iff$$

$$\iff \begin{cases} \text{span}(A^1, \dots, A^n) = K^n \iff A^1, \dots, A^n \text{ sono base di } K^n \\ \text{span}(A_1, \dots, A_n) = K^n \iff A_1, \dots, A_n \text{ sono base di } K^n \end{cases}$$

- 1) \iff 2)

– Supponiamo che $\exists! B = (B^1, \dots, B^n) \in \text{Mat}_{n \times n}(K) \mid A \cdot B = B \cdot A = I_n$. Per definizione di prodotto tra matrici ne segue che:

$$AB = I_n \iff AB^1 = e_1, AB^2 = e_2, \dots, AB^n = e_n \iff$$

$$\iff L_A(B^1) = e_1, L_A(B^2) = e_2, \dots, L_A(B^n) = e_n \iff$$

$$\iff e_1, e_2, \dots, e_n \in \text{im}(L_A) \iff \text{im}(L_A) = \text{span}(e_1, \dots, e_n) = K^n \iff$$

$$\iff \text{rk}(A) = n$$

- 2) \iff 6)
 - Se $\text{rk}(A) = n$, è possibile ridurre a scala A fino ad ottenere I_n
 - Viceversa, poiché $\text{rk}(I_n) = n$, se I_n è equivalente per righe e colonne ad A ne segue automaticamente che $\text{rk}(A) = n$

□

Corollario 29

È possibile definire il **gruppo generale lineare** anche come:

$$GL(n, K) = \{A \in \text{Mat}_{n \times n}(K) \mid \det(A) \neq 0\}$$

Osservazione 63

Data una matrice $A \in \text{Mat}_{n \times n}(K)$, si ha che:

$$\det(A^{-1}) = \det(A)^{-1}$$

Dimostrazione:

- Per il teorema di Binet, si ha che:

$$1 = \det(I_n) = \det(A \cdot A^{-1}) = \det(A) \det(A^{-1}) \implies \det(A)^{-1} = \det(A^{-1})$$

□

Definizione 93: Gruppo speciale lineare

Dato il gruppo $(GL(n, K), \cdot)$, definiamo $SL(n, K) \trianglelefteq GL(n, K)$ come **gruppo speciale lineare**, dove

$$SL(n, K) = \{A \in GL(n, K) \mid \det(A) = 1\}$$

Dimostrazione:

- $SL(n, K) \leq GL(n, K)$
 - $\det(I_n) = 1 \implies I_n \in SL(n, K)$
 - $A, B \in SL(n, K) \implies \det(AB) = \det(A) \det(B) = 1 \cdot 1 = 1 \implies AB \in SL(n, K)$
 - $A \in SL(n, K) \implies \det(A^{-1}) = \det(A)^{-1} = 1 \implies A^{-1} \in SL(n, K)$
- Date le matrici $A, B \in SL(n, K)$, si ha che:

$$\begin{aligned} A \sim_L B &\iff A^{-1}B \in SL(n, K) \iff \det(A^{-1}B) = 1 \iff \det(A^{-1}) \det(B) = 1 \iff \\ &\iff \det(A)^{-1} \det(B) = 1 \iff \det(A)^{-1} = \det(B)^{-1} \iff \det(A) = \det(B) \end{aligned}$$

$$\begin{aligned}
A \sim_R B &\iff AB^{-1} \in SL(n, K) \iff \det(AB^{-1}) = 1 \iff \det(A) \det(B^{-1}) = 1 \iff \\
&\iff \det(A) \det(B)^{-1} = 1 \iff \det(B)^{-1} = \det(A)^{-1} \iff \det(B) = \det(A)
\end{aligned}$$

dunque le classi laterali sinistre e destre coincidono, implicando che $SL(n, K) \trianglelefteq GL(n, K)$

□

Osservazione 64

Data una matrice $A \in GL(n, K)$, poiché è A invertibile se e solo se equivalente per righe e colonne a I_n , si ha che

$$(A \mid I_n), (I_n \mid B) \text{ equivalenti per righe} \iff B = A^{-1}$$

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:

$$\begin{aligned}
(A \mid I_n) &= \left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 3 & 4 & 0 & 1 \end{array} \right) \xrightarrow{R_2 - 3R_1} \left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & -2 & -3 & 1 \end{array} \right) \\
&\xrightarrow{R_1 + R_2} \left(\begin{array}{cc|cc} 1 & 0 & -2 & 1 \\ 0 & -2 & -3 & 1 \end{array} \right) \xrightarrow{-\frac{1}{2}R_2} \left(\begin{array}{cc|cc} 1 & 0 & -2 & 1 \\ 0 & 1 & \frac{3}{2} & -\frac{1}{2} \end{array} \right) = (I_n \mid B) \\
&\implies A^{-1} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix}
\end{aligned}$$

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:

$$(A \mid I_N) = \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 4 & 5 & 6 & 0 & 1 & 0 \\ 7 & 8 & 0 & 0 & 0 & 1 \end{array} \right) \xrightarrow{R_2 - 4R_1} \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -4 & 1 & 0 \\ 7 & 8 & 0 & 0 & 0 & 1 \end{array} \right)$$

$$\begin{aligned}
& \xrightarrow{R_3+7R_1} \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -4 & 1 & 0 \\ 0 & -6 & -21 & -7 & 0 & 1 \end{array} \right) \xrightarrow{R_3-2R_2} \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -4 & 1 & 0 \\ 0 & 0 & -9 & 1 & -2 & 1 \end{array} \right) \\
& \xrightarrow{R_2*=-\frac{1}{3}} \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & \frac{4}{3} & -\frac{1}{3} & 0 \\ 0 & 0 & -9 & 1 & -2 & 1 \end{array} \right) \xrightarrow{-\frac{1}{9}R_3} \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & \frac{4}{3} & -\frac{1}{3} & 0 \\ 0 & 0 & 1 & -\frac{1}{9} & \frac{2}{9} & -\frac{1}{9} \end{array} \right) \\
& \xrightarrow{R_1-2R_2} \left(\begin{array}{ccc|ccc} 1 & 0 & -1 & -\frac{5}{3} & \frac{2}{3} & 0 \\ 0 & 1 & 2 & \frac{4}{3} & -\frac{1}{3} & 0 \\ 0 & 0 & 1 & -\frac{1}{9} & \frac{2}{9} & -\frac{1}{9} \end{array} \right) \xrightarrow{R_1+R_3} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -\frac{16}{9} & \frac{8}{9} & -\frac{1}{9} \\ 0 & 1 & 2 & \frac{4}{3} & -\frac{1}{3} & 0 \\ 0 & 0 & 1 & -\frac{1}{9} & \frac{2}{9} & -\frac{1}{9} \end{array} \right) \\
& \xrightarrow{R_2-2R_3} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -\frac{16}{9} & \frac{8}{9} & -\frac{1}{9} \\ 0 & 1 & 0 & \frac{14}{9} & -\frac{7}{9} & \frac{2}{9} \\ 0 & 0 & 1 & -\frac{1}{9} & \frac{2}{9} & -\frac{1}{9} \end{array} \right) \Rightarrow A^{-1} = \left(\begin{array}{ccc} -\frac{16}{9} & \frac{8}{9} & -\frac{1}{9} \\ \frac{14}{9} & -\frac{7}{9} & \frac{2}{9} \\ -\frac{1}{9} & \frac{2}{9} & -\frac{1}{9} \end{array} \right) \Rightarrow \\
& \Rightarrow A^{-1} = \frac{1}{9} \begin{pmatrix} -16 & 8 & -1 \\ 14 & -7 & 2 \\ -1 & 2 & -1 \end{pmatrix}
\end{aligned}$$

dove $\det(A^{-1}) = \frac{1}{27}$

Definizione 94: 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:

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix} \Rightarrow A^T = \begin{pmatrix} 1 & 5 & 9 \\ 2 & 6 & 10 \\ 3 & 7 & 11 \\ 4 & 8 & 12 \end{pmatrix}$$

Osservazione 65

Date due matrici $A, B \in \text{Mat}_{n \times n}(K)$, si verifica che:

- $\det(A) = \det(A^T)$
- $(AB)^T = B^T A^T$

(dimostrazioni omessa)

Definizione 95: Matrice dei cofattori

Data una matrice $A \in \text{Mat}_{n \times n}(K)$, definiamo come **matrice dei cofattori** la matrice $\text{cof}(A) \in \text{Mat}_{n \times n}(K)$ avente come entrate i cofattori di ogni entrata della matrice A

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} \implies \text{cof}(A) = \begin{pmatrix} \text{cof}(A)_{1,1} & \cdots & \text{cof}(A)_{1,n} \\ \vdots & \ddots & \vdots \\ \text{cof}(A)_{n,1} & \cdots & \text{cof}(A)_{n,n} \end{pmatrix}$$

dove ricordiamo che

$$\text{cof}(A)_{i,j} = (-1)^{i+j} \cdot \det(M_{i,j})$$

Definizione 96: Matrice aggiunta

Data una matrice $A \in \text{Mat}_{n \times n}(K)$, definiamo come **matrice aggiunta** la trasposta della matrice dei cofattori di A :

$$\text{adj}(A) = (\text{cof}(A))^T$$

Teorema 34: Inversa di una matrice tramite aggiunta

Data una matrice $A \in \text{Mat}_{n \times n}(K)$ dove $\det(A) \neq 0$, si verifica che:

$$A^{-1} = \frac{1}{\det(A)} \cdot \text{adj}(A)$$

Dimostrazione:

- Come conseguenza dello sviluppo di Laplace, si verifica che:

$$\begin{aligned} A \cdot \text{adj}(A) &= \text{adj}(A) \cdot A = \det(A) \cdot I_n \implies \text{adj}(A) \cdot A = \det(A) \cdot I_n \implies \\ &\implies \text{adj}(A) = \det(A) \cdot I_n \cdot A^{-1} \implies \det(A)^{-1} \text{adj}(A) = A^{-1} \end{aligned}$$

□

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:

$$\text{cof}(A) = \begin{pmatrix} \text{cof}_{1,1}(A) & \text{cof}_{1,2}(A) & \text{cof}_{1,3}(A) \\ \text{cof}_{2,1}(A) & \text{cof}_{2,2}(A) & \text{cof}_{2,3}(A) \\ \text{cof}_{3,1}(A) & \text{cof}_{3,2}(A) & \text{cof}_{3,3}(A) \end{pmatrix} = \begin{pmatrix} -48 & 42 & -3 \\ 24 & -21 & 6 \\ -3 & 6 & -3 \end{pmatrix}$$

mentre la conseguente matrice aggiunta corrisponde a:

$$\text{adj}(A) = \begin{pmatrix} -48 & 24 & -3 \\ 42 & -21 & 6 \\ -3 & 6 & -3 \end{pmatrix}$$

- Dunque, la matrice inversa di A corrisponde a:

$$A^{-1} = \frac{1}{27} \begin{pmatrix} -48 & 24 & -3 \\ 42 & -21 & 6 \\ -3 & 6 & -3 \end{pmatrix} = \frac{1}{9} \begin{pmatrix} -16 & 8 & -1 \\ 14 & -7 & 2 \\ -1 & 2 & -1 \end{pmatrix}$$

Corollario 30

Data una matrice $A \in \text{Mat}_{2 \times 2}(K)$, 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:

$$\text{cof}(A) = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \implies \text{adj}(A) = (\text{cof}(A))^T = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

- Di conseguenza, la sua inversa sarà:

$$A^{-1} = \frac{1}{\det(A)} \cdot \text{adj}(A) = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

9.5 Teorema degli orlati

Definizione 97: Orlato di un minore

Data una matrice $A \in \text{Mat}_{m \times n}(K)$ e dati un suo minore M di ordine k e un minore M' di ordine $k+1$, definiamo M' come **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:

$$M'_1 = \begin{pmatrix} 1 & 3 & 4 \\ 5 & 7 & 8 \\ 9 & 11 & 12 \end{pmatrix} \quad M'_2 = \begin{pmatrix} 1 & 2 & 3 \\ 5 & 6 & 7 \\ 9 & 10 & 11 \end{pmatrix}$$

Osservazione 66

Data una matrice $A \in \text{Mat}_{m \times n}(K)$ e un suo minore M di ordine k , esistono $(m-k)(n-k)$ orlati di M in A

Teorema 35: Teorema degli orlati (o di Kronecker)

Data una matrice $A \in \text{Mat}_{m \times n}(K)$, si ha che:

$$\text{rk}(A) = k \iff \exists M \text{ minore di } A \mid \begin{cases} \text{ordine di } M = k \\ \det(M) \neq 0 \\ \det(M') = 0, \forall M' \text{ orlato di } M \end{cases}$$

(dimostrazione omessa)

Esempi:

1. • Vogliamo discutere il comportamento di tale sistema al variare dei parametri $a, b \in \mathbb{R}$:

$$\begin{cases} ax + y + z = 1 \\ x + ay + z = 0 \\ x + y + az = b \end{cases} \implies A_b = \left(\begin{array}{ccc|c} a & 1 & 1 & 1 \\ 1 & a & 1 & 0 \\ 1 & 1 & a & b \end{array} \right) \implies$$

$$\implies \begin{cases} \text{rk}(A_b) = \text{rk}(A) & \text{se } \dim(A^1, \dots, A^n, b) = \dim(A^1, \dots, A^n) \\ \text{rk}(A_b) = \text{rk}(A) + 1 & \text{se } \dim(A^1, \dots, A^n, b) \neq \dim(A^1, \dots, A^n) \end{cases}$$

- 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 $\text{rk}(A) = 3$.

Inoltre, siccome $\text{rk}(A_b) \leq \min(3, 4) = 3$ e siccome $\text{rk}(A_b) = \text{rk}(A)$ oppure $\text{rk}(A_b) = \text{rk}(A) + 1$, allora ne segue necessariamente che $\text{rk}(A) = \text{rk}(A_b) = 3$.

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::

$$A_b = \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & b \end{array} \right) \xrightarrow{R_2+=-R_1} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & -1 \\ 1 & 1 & 1 & b \end{array} \right)$$

$$\xrightarrow{R_3+=-R_1} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & b-1 \end{array} \right) \xrightarrow{R_3+=-R_2} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & b \end{array} \right)$$

$$\xrightarrow{R_3+=b \cdot R_2} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{array} \right)$$

implicando che $\text{rk}(A) = 1$ e $\text{rk}(A_b) = 2$, 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 $\text{rk}(A) = 2$

$$A = \begin{pmatrix} -2 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{pmatrix} \implies \text{rk}(A) = 2$$

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:

$$\text{rk}(A) = \begin{cases} 2 & \text{se } a = -2, b = -1 \implies \text{rk}(A) = \text{rk}(A_b) \implies \exists \text{ inf. soluzioni} \\ 3 & \text{se } a = -2, b \neq -1 \implies \text{rk}(A) \neq \text{rk}(A_b) \implies \nexists \text{ soluzioni} \end{cases}$$

- In particolare, se $a = -2$ e $b = -1$, possiamo trovare le infinite soluzioni del sistema in funzione di x :

$$\begin{cases} -2x + y + z = 1 \\ x - 2y + z = 0 \\ x + y - 2z = -1 \end{cases} \implies \begin{cases} -2y + z = -x \\ y - 2z = 1 - x \end{cases}$$

appliciamo 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 $n - \text{rk}(A) = 3 - 2 = 1$)

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

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in V \iff \text{rk}(A) = \text{rk} \begin{pmatrix} 1 & 4 & x-1 \\ 2 & 5 & y \\ 3 & 6 & z+1 \end{pmatrix} = 2$$

- 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:

$$\text{rk}(A) = \begin{cases} 2 & \text{se } \det(A) = 0 \\ 3 & \text{se } \det(A) \neq 0 \end{cases}$$

- Dunque, si ha che:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in V \iff \text{rk}(A) = 2 \iff \det(A) = 0$$

- Utilizzando lo sviluppo di Laplace sulla terza colonna, si ha che:

$$\det(A) = 0 \iff (x-1) \cdot \det \begin{pmatrix} 2 & 5 \\ 3 & 6 \end{pmatrix} - y \cdot \det \begin{pmatrix} 1 & 4 \\ 3 & 6 \end{pmatrix} + (z-1) \cdot \det \begin{pmatrix} 1 & 4 \\ 2 & 5 \end{pmatrix} = 0$$

$$\iff -3(x-1) + 6y - 3(z+1) \iff -3x + 6y - 3z = 0 \iff x - 2y + z = 0$$

- 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

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 omesso*), 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 descriventi π :

$$\begin{aligned} \pi = \begin{cases} x = 4 - 2b + 5c \\ y = 3b - c \\ z = 1 + b - 2c \end{cases} & \iff \begin{pmatrix} x - 4 \\ y \\ z - 1 \end{pmatrix} = b \begin{pmatrix} -2 \\ 3 \\ 1 \end{pmatrix} + c \begin{pmatrix} 5 \\ -1 \\ -2 \end{pmatrix} \iff \\ & \iff \text{rk} \begin{pmatrix} -2 & 5 & x - 4 \\ 3 & -1 & y \\ 1 & -2 & z - 1 \end{pmatrix} = 2 \end{aligned}$$

Siccome $\det(M_{3,3}) = -13 \neq 0$, per il teorema degli orlati, si ha che:

$$\begin{aligned} \Leftrightarrow \operatorname{rk} \begin{pmatrix} -2 & 5 & x-4 \\ 3 & -1 & y \\ 1 & -2 & z-1 \end{pmatrix} = 2 &\Leftrightarrow \det \begin{pmatrix} -2 & 5 & x-4 \\ 3 & -1 & y \\ 1 & -2 & z-1 \end{pmatrix} = 0 \Leftrightarrow \\ (x-4)(-5) - y(-1) + (z-1)(-13) = 0 &\Leftrightarrow 5x - y + 13z = 33 \end{aligned}$$

Siccome $x \in r \cap \pi \Leftrightarrow x \in r \wedge x \in \pi$, sostituendo i valori assunti da x, y e z nell'equazione cartesiana di π otteniamo che:

$$-5x + y - 13z = 33 \Leftrightarrow 5(-2+3a) - (1-2a) + 13(5a) = 33 \Leftrightarrow a = \frac{22}{41}$$

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 descriventi π e il sistema di equazioni cartesiane descriventi r .

Sappiamo già che:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \pi \Leftrightarrow 5x - y + 13z = 33$$

dunque ricaviamo le equazioni cartesiane di r :

$$\begin{aligned} r = \begin{cases} x = -2 + 3a \\ y = 1 - 2a \\ z = 5a \end{cases} &\Leftrightarrow \begin{pmatrix} x+2 \\ y-1 \\ z \end{pmatrix} = a \begin{pmatrix} 3 \\ -2 \\ 5 \end{pmatrix} \Leftrightarrow \\ &\Leftrightarrow \operatorname{rk} \begin{pmatrix} 3 & x+2 \\ -2 & y-1 \\ 5 & z \end{pmatrix} = 1 \end{aligned}$$

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:

$$\begin{aligned} \operatorname{rk} \begin{pmatrix} 3 & x+2 \\ -2 & y-1 \\ 5 & z \end{pmatrix} = 1 &\Leftrightarrow \begin{cases} \det \begin{pmatrix} 3 & x+2 \\ -2 & y-1 \end{pmatrix} = 0 \\ \det \begin{pmatrix} 3 & x+2 \\ 5 & z \end{pmatrix} = 0 \end{cases} \Leftrightarrow \\ &\Leftrightarrow \begin{cases} 2x + 3y + 1 = 0 \\ -5x + 3z - 10 = 0 \end{cases} \end{aligned}$$

Possiamo quindi costruire un nuovo sistema di equazioni cartesiane corrispondente a $r \cap \pi$ utilizzando le due equazioni cartesiane descriventi 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

9.6 Matrici simili

Definizione 98: Matrici simili

Date due matrici $A, B \in \text{Mat}_{n \times n}(K)$, tali matrici vengono dette **simili** se si verifica che:

$$\exists C \in GL(n, K) \mid A = C^{-1}BC$$

Attenzione: tale condizione non è equivalente ad affermare che A è coniugato a B , poiché nella relazione di coniugio gli elementi C, C^{-1} dovrebbero essere presi in $\text{Mat}_{n \times n}(K)$ e non in $GL(n, K)$. Inoltre, ricordiamo che $GL(n, K) \not\subseteq \text{Mat}_{n \times n}(K)$.

Proposizione 62: Determinante invariante

Date due matrici $A, B \in \text{Mat}_{n \times n}(K)$, se A è simile a B , 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:

$$\det(B) = \det(C^{-1}AC) = \det(C^{-1}) \det(A) \det(C) = \det(C)^{-1} \det(A) \det(C) = \det(A)$$

□

Definizione 99: Traccia di una matrice

Data una matrice $A \in \text{Mat}_{n \times n}(K)$, definiamo come **traccia** di A la somma delle entrate sulla diagonale principale:

$$\text{tr}(A) = \sum_{k=1}^n a_{k,k}$$

Lemma 20

Date $A \in \text{Mat}_{m \times n}(K)$ e $B \in \text{Mat}_{n \times m}(K)$, si verifica che:

$$\text{tr}(AB) = \text{tr}(BA)$$

Dimostrazione:

- Il risultato segue dalla definizione stessa di prodotto tra matrici:

$$\text{tr}(AB) = \sum_{k=1}^n (ab)_{k,k} = \sum_{k=1}^n \sum_{j=1}^m a_{k,j} b_{j,k} = \sum_{j=1}^m \sum_{k=1}^n b_{j,k} a_{k,j} = \sum_{k=1}^n (ba)_{k,k} = \text{tr}(BA)$$

□

Proposizione 63: Traccia invariante

Date due matrici $A, B \in \text{Mat}_{n \times n}(K)$, se A è simile a B , allora

$$\text{tr}(A) = \text{tr}(B)$$

Dimostrazione:

- Se $\exists C \in GL(n, K) \mid B = C^{-1}AC$, allora

$$\text{tr}(B) = \text{tr}(C^{-1}AC) = \text{tr}(C^{-1}CA) = \text{tr}(A)$$

□

Definizione 100: Polinomio caratteristico

Data una matrice $A \in \text{Mat}_{n \times n}(K)$, 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:

$$p_A(x) = \det \begin{pmatrix} x-1 & 0 & +1 \\ -2 & x+3 & 0 \\ -1 & 0 & x-1 \end{pmatrix} = (x-3)(x^2 - 2x + 2)$$

Proposizione 64: Polinomio invariante

Date due matrici $A, B \in \text{Mat}_{n \times n}(K)$, se A è simile a B , allora

$$p_A(x) = p_B(x)$$

Dimostrazione:

- Se $\exists C \in GL(n, K) \mid B = C^{-1}AC$, allora

$$\begin{aligned} p_B(x) &= \det(xI_n - B) = \det(xI_n - C^{-1}AC) = \det(xC^{-1}C - C^{-1}AC) = \\ &= \det(C^{-1}xI_nC - C^{-1}AC) = \det(C^{-1}(xI_n - A)C) = \det(C^{-1}) \det(xI_n - A) \det(C) = \\ &= \det(C)^{-1} \det(xI_n - A) \det(C) = \det(xI_n - A) = p_A(x) \end{aligned}$$

□

Osservazione 67

Data una matrice $A \in \text{Mat}_{n \times n}(K)$, si verifica che:

$$p_A(x) = x^n - \text{tr}(A)x^{n-1} + \dots + (-1)^n \det(A)$$

(dimostrazione omessa)

Definizione 101: Autovalori ed Autovettori

Data $A \in \text{Mat}_{n \times n}(K)$ e uno scalare $\lambda \in K$, le seguenti condizioni sono equivalenti:

1. $p_A(\lambda) = 0$
2. $\exists v \neq 0_{K^n} \in K^n \mid Av = \lambda v$

Dove λ viene detto **autovalore di A** e v viene detto **autovettore relativo a λ**

Dimostrazione:

- Supponiamo quindi che esista $\exists v \neq 0_{K^n} \in K^n \mid Av = \lambda v$:

$$\begin{aligned} \exists v \neq 0_{K^n} \in K^n \mid (\lambda I_n - A)v = 0 &\iff \ker(L_{(\lambda I_n - A)}) \neq \{0_{K^n}\} \iff \\ \iff \dim(\ker(L_{(\lambda I_n - A)})) > 0 &\iff \operatorname{rk}(\lambda I_n - A) = n - \dim(\ker(L_{(\lambda I_n - A)})) < n \\ \iff \det(\lambda I_n - A) = 0 &\iff p_A(\lambda) = 0 \end{aligned}$$

□

Osservazione 68

Data $A \in \operatorname{Mat}_{n \times n}(K)$ e uno scalare $\lambda \in K$, il vettore $v \neq 0_{K^n} \in K^n$ è un autovettore relativo a λ se e solo se:

$$(A - \lambda I_n)v = 0$$

o in alternativa

$$0 = (\lambda I_n - A)v$$

Dimostrazione:

- Notiamo facilmente che:

$$\exists v \neq 0 \in K^n \mid Av = \lambda v \iff \begin{cases} 0 = \lambda v - Av \iff 0 = (\lambda I_n - A)v \\ Av - \lambda v = 0 \iff (A - \lambda I_n)v = 0 \end{cases}$$

□

Definizione 102: Spettro e Autospazio relativo

Data una matrice $A \in \operatorname{Mat}_{n \times n}(K)$, definiamo come **spettro** di A l'insieme dei suoi autovalori

$$\operatorname{sp}(A) = \{\lambda \in K \mid p_A(\lambda) = 0\}$$

e come **autospazio relativo a $\lambda \in \operatorname{sp}(A)$** il sottospazio di K^n generato dagli autovettori relativi a λ :

$$E_\lambda(A) = \{v \in K^n \mid Av = \lambda v\}$$

Proposizione 65: Spettro invariante

Date due matrici $A, B \in \operatorname{Mat}_{n \times n}(K)$, se A è simile a B , allora

$$\operatorname{sp}(A) = \operatorname{sp}(B)$$

Inoltre, dato $\lambda \in \operatorname{sp}(A) = \operatorname{sp}(B)$ si ha che:

$$E_\lambda(A) = E_\lambda(B) \iff A = B$$

Dimostrazioni:

- Se $\exists C \in GL(n, K) \mid B = C^{-1}AC$, allora $p_A(x) = p_B(x)$, dunque si ha che:

$$\mu \in \text{sp}(A) \iff p_A(\mu) = p_B(\mu) = 0 \iff \mu \in \text{sp}(B)$$

- Dato $\lambda \in \text{sp}(A) = \text{sp}(B)$, si ha che:

$$E_\lambda(A) = E_\lambda(B) \iff Av = \lambda v = Bv, \forall v \in E_\lambda(A) \iff A = B$$

□

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 $\text{sp}(A) = \{0, 1, 2\}$

- Gli autovettori dell'autospazio $E_0(A)$ corrispondono a:

$$v = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in E_0(A) \iff (0 \cdot I_n - A)v = 0 \iff \begin{cases} -x - y - 3z = 0 \\ -x + 5z = 0 \\ 2x + y - 2z = 0 \end{cases} \iff$$

$$\iff \begin{cases} x = 5t \\ y = -8t \\ z = t \end{cases} \iff \begin{pmatrix} x \\ y \\ z \end{pmatrix} = t \begin{pmatrix} 5 \\ -8 \\ 1 \end{pmatrix}$$

- Gli autovettori dell'autospazio $E_1(A)$ corrispondono a:

$$v = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in E_1(A) \iff (1 \cdot I_n - A)v = 0 \iff \begin{cases} -y - 3z = 0 \\ -x + y + 5z = 0 \\ 2x + y - z = 0 \end{cases} \iff$$

$$\iff \begin{cases} x = 2t \\ y = -3t \\ z = t \end{cases} \iff \begin{pmatrix} x \\ y \\ z \end{pmatrix} = t \begin{pmatrix} 2 \\ -3 \\ 1 \end{pmatrix}$$

- Gli autovettori dell'autospazio $E_2(A)$ corrispondono a:

$$v = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in E_0(A) \iff (2 \cdot I_n - A)v = 0 \iff \begin{cases} x - y - 3z = 0 \\ -x + 2y + 5z = 0 \\ 2x + y = 0 \end{cases} \iff$$

$$\iff \begin{cases} x = t \\ y = -2t \\ z = t \end{cases} \iff \begin{pmatrix} x \\ y \\ z \end{pmatrix} = t \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}$$

Definizione 103: Molteplicità algebrica e geometrica

Data una matrice $A \in \text{Mat}_{n \times n}(K)$, per ogni autovalore $\lambda \in \text{sp}(A)$ 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:

$$\nu(\lambda) = \dim(E_\lambda(A)) = n - \text{rk}(\lambda I_n - A)$$

Per ogni $\lambda \in \text{sp}(A)$, si verifica che:

$$1 \leq \nu(\lambda) \leq \mu(\lambda)$$

Proposizione 66: Molteplicità invarianti

Se $A, B \in \text{Mat}_{n \times n}(K)$ sono matrici simili, allora $\forall \lambda \in \text{sp}(A) = \text{sp}(B)$ si ha che:

$$\mu_A(\lambda) = \mu_B(\lambda) \qquad \nu_A(\lambda) = \nu_B(\lambda)$$

(dimostrazione omessa)

9.6.1 Diagonalizzazione di una matrice

Definizione 104: Matrice diagonale

Sia $A \in \text{Mat}_{n \times n}(K)$. 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

$$A = \begin{pmatrix} a_{1,1} & 0 & \cdots & \cdots & 0 \\ 0 & a_{2,2} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_{n-1,n-1} & 0 \\ 0 & \cdots & \cdots & 0 & a_{n,n} \end{pmatrix}$$

Definizione 105: Matrici triangolarizzabili e diagonalizzabili

Una matrice $A \in \text{Mat}_{n \times n}(K)$ viene detta **triangolarizzabile** se simile ad una matrice triangolare $T \in \text{Mat}_{n \times n}(K)$, mentre viene detta **diagonalizzabile** se simile ad una matrice diagonale $D \in \text{Mat}_{n \times n}(K)$

Proposizione 67

Data una matrice $A \in \text{Mat}_{n \times n}(K)$, le seguenti condizioni sono equivalenti:

1. A è triangolarizzabile
2. La somma di tutte le sue molteplicità algebriche è n :

$$\sum_{\lambda \in \text{sp}(A)} \mu(\lambda) = n = \dim(K^n)$$

3. Il suo polinomio caratteristico è completamente fattorizzabile:

$$p_A(x) = \prod_{\lambda \in \text{sp}(A)} (x - \lambda)^{\mu(\lambda)}$$

(dimostrazione omessa)

Corollario 31

Per il teorema fondamentale dell'algebra, **ogni matrice** $A \in \text{Mat}_{n \times n}(K)(\mathbb{C})$ è **triangolarizzabile**.

Analogamente, una matrice $B \in \text{Mat}_{n \times n}(\mathbb{R})$ è **triangolarizzabile** se e solo se

$$\forall \lambda \in \text{sp}(B), \lambda \in \mathbb{R} \iff \text{sp}(B) \subseteq \mathbb{R}$$

Esempio:

- Data la matrice

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \text{Mat}_{2 \times 2}(\mathbb{R})$$

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
- Considerando invece la matrice $A' \in \text{Mat}_{2 \times 2}(\mathbb{C})$ avente entrate coincidenti a quelle di A , otteniamo che:

$$p_{A'}(x) = (x - i)(x + i) \in \mathbb{C}[x] \implies \text{sp}(A') = \{\pm i\} \subseteq \mathbb{C}$$

dunque A' è triangolarizzabile

Proposizione 68

Data una matrice $A \in \text{Mat}_{n \times n}(K)$, le seguenti condizioni sono equivalenti:

1. A è diagonalizzabile
2. La somma di tutte le sue molteplicità geometriche è n :

$$\sum_{\lambda \in \text{sp}(A)} \nu(\lambda) = n = \dim(K^n)$$

3. Esistono B^1, \dots, B^n autovettori di A tali che:

$$B^1, \dots, B^n \text{ base di } K^n$$

4. Il suo spettro contiene n autovalori diversi tra loro:

$$|\text{sp}(A)| = n$$

Osservazione 69

Data una matrice $A \in \text{Mat}_{n \times n}(K)$, dati $\lambda, \mu \in \text{sp}(A) \mid \lambda \neq \mu$ si ha che:

$$E_\lambda(A) \cap E_\mu(A) = \{0_{K^n}\}$$

Dimostrazione:

- Ovviamente, essendo sottospazi vettoriali, si ha che:

$$0_{K^n} \in E_\lambda(A), 0_{K^n} \in E_\mu(A) \implies 0_{K^n} \in E_\lambda(A) \cap E_\mu(A)$$

- Supponiamo quindi che $\exists v \neq 0_{K^n} \in K^n \mid \lambda v = Av = \mu v$, dunque un autovettore relativo sia λ sia a μ , dove $\lambda \neq \mu$. Ne segue che:

$$\lambda v = Av = \mu v \implies \lambda v = \mu v \implies (\lambda - \mu)v = 0_{K^n}$$

- Poiché $\lambda \neq \mu \implies \lambda - \mu \neq 0$, si ha che:

$$(\lambda - \mu)v = 0_{K^n} \iff v = 0_{K^n}$$

contraddicendo quindi l'ipotesi iniziale, dunque l'unica possibilità è che:

$$\nexists v \neq 0_{K^n} \mid v \in E_\lambda(A), v \in E_\mu(A) \iff E_\lambda(A) \cap E_\mu(A) = \{0_{K^n}\}$$

□

Corollario 32

Data una matrice $A \in \text{Mat}_{n \times n}(K)$ e dati i vettori $v_1 \neq 0_{K^n} \in E_{\lambda_1}(A), \dots, v_k \neq 0_{K^n} \in E_{\lambda_k}(A)$, dove $\lambda_i \neq \lambda_j, \forall i \neq j$, si ha che:

$$v_1, \dots, v_k \text{ linearmente indipendenti}$$

Dimostrazione:

- Poiché:

$$\lambda, \mu \in \text{sp}(A) \mid \lambda \neq \mu \implies E_\lambda(A) \cap E_\mu(A) = \{0_{K^n}\}$$

ne segue automaticamente che:

$$v_i \neq 0_{K^n} \in E_{\lambda_i}(A) \implies v_i \neq 0_{K^n} \notin E_{\lambda_j}(A), \forall j \neq i$$

dunque v_1, \dots, v_k sono linearmente indipendenti

□

Proposizione 69: Matrice diagonalizzante

Data una matrice $A \in \text{Mat}_{n \times n}(K)$, se esiste una base $B^1, \dots, B^i, \dots, B^j, \dots, B^n$ di K^n tale che:

- B^1, \dots, B^i è base di $E_{\lambda_1}(A)$
- \vdots
- B^j, \dots, B^n è base di $E_{\lambda_n}(A)$

dove $\lambda_1, \dots, \lambda_n \in \text{sp}(A)$ e dove $i \neq j$ allora:

$$\exists B = (B^1, \dots, B^i, \dots, B^j, \dots, B^n) \in GL(n, K) \mid D = B^{-1}AB$$

dove $D \in \text{Mat}_{n \times n}(K)$ è una matrice diagonale e dove B viene detta **matrice diagonalizzante**.

Esempio:

1. • Consideriamo la seguente matrice

$$A = \begin{pmatrix} 5 & -8 & 3 \\ 4 & -8 & 4 \\ 5 & -12 & 7 \end{pmatrix} \in \text{Mat}_{3 \times 3}(\mathbb{R})$$

- Il suo polinomio caratteristico corrisponde a:

$$p_A(x) = \det \begin{pmatrix} x-5 & 8 & -3 \\ -4 & x+8 & -4 \\ -5 & 12 & x-7 \end{pmatrix} =$$

$$= (x-5) \det \begin{pmatrix} x+8 & -4 \\ 12 & x-7 \end{pmatrix} + 4 \det \begin{pmatrix} 8 & -3 \\ 12 & x-7 \end{pmatrix} - 5 \det \begin{pmatrix} 8 & -3 \\ x+8 & -4 \end{pmatrix} =$$

$$= (x-5)(x^2 + x - 8) + 4(8x - 20) - 5(3x - 8) = x^3 - 4x^2 + 4x = x(x-2)^2$$

dunque sappiamo che A è triangolarizzabile e che il suo spettro è $\text{sp}(A) = \{0, 2\}$.

- 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:

$$\nu(2) = 2 = \dim(E_2(A)) = 3 - \text{rk}(2 \cdot I_n - A) = \iff \text{rk}(2 \cdot I_n - A) = 1$$

- Tuttavia, considerando il minore $M_{3,3}$, per il teorema degli orlati si verifica che:

$$\det \begin{pmatrix} -3 & 8 \\ -4 & 10 \end{pmatrix} = -30 + 32 = 2 \neq 0 \implies \text{rk}(2 \cdot I_n - A) \geq 2$$

Dunque si ha che $\text{rk}(2 \cdot I_n - A) \neq 1$, implicando quindi che A non sia diagonalizzabile.

- Difatti, si ha che:

$$1 \leq \nu(2) = 3 - \text{rk}(2 \cdot I_n - A) \leq 3 - 2 = 1 \iff \nu(2) = 1$$

e dunque che:

$$\nu(0) + \nu(2) = 1 + 1 = 2 \neq 3 = \dim(\mathbb{R}^3)$$

- Consideriamo la seguente matrice

$$A = \begin{pmatrix} 1 & k \\ 2 & k-1 \end{pmatrix} \in \text{Mat}_{2 \times 2}(\mathbb{R})$$

- 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 $\text{sp}(A) = \{-1, k+1\}$

- Siccome $p_A(x)$ è completamente fattorizzabile indipendentemente dal valore assunto da k , allora A è sempre triangolarizzabile.
- Se $k = -2$, si ha che:

$$A = \begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix} \implies p_A(x) = (x+1)^2 \implies \text{sp}(A) = \{-1\}$$

Dunque A è diagonalizzabile se e solo se $\nu(-1) = 2$.

Tuttavia, considerando il sistema $(-1 \cdot I_n - A)v = 0$, notiamo che :

$$\begin{aligned} \begin{cases} -2x + 2y = 0 \\ -2x + 2y = 0 \end{cases} &\iff \begin{cases} x = t \\ y = t \end{cases} \iff \\ \iff \begin{pmatrix} x \\ y \end{pmatrix} = t \begin{pmatrix} 1 \\ 1 \end{pmatrix} &\implies \nu(-1) = \dim(E_{-1}(A)) = 1 \end{aligned}$$

Dunque A non è diagonalizzabile se $k = -2$

- Se invece $k \neq -2$, si ha che:

$$p_A(x) = (x+1)(x-k-1) \implies \text{sp}(A) = \{-1, k+1\}$$

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 :

$$\begin{aligned} \begin{cases} -2x + ky = 0 \\ -2x + ky = 0 \end{cases} &\iff \begin{cases} x = t \\ y = -\frac{k}{2} \end{cases} \iff \\ \iff \begin{pmatrix} x \\ y \end{pmatrix} = t \begin{pmatrix} 1 \\ -\frac{k}{2} \end{pmatrix} &\implies \nu(-1) = \dim(E_{-1}(A)) = 1 \end{aligned}$$

mentre per il sistema $((k+1) \cdot I_n - A)v = 0$ si ha che :

$$\begin{aligned} \begin{cases} kx - ky = 0 \\ -2x + 2y = 0 \end{cases} &\iff \begin{cases} x = t \\ y = t \end{cases} \iff \\ \iff \begin{pmatrix} x \\ y \end{pmatrix} = t \begin{pmatrix} 1 \\ 1 \end{pmatrix} &\implies \nu(k+1) = \dim(E_{k+1}(A)) = 1 \end{aligned}$$

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 :

$$B = \begin{pmatrix} 1 & 1 \\ -\frac{k}{2} & 1 \end{pmatrix} \implies D = B^{-1}AB \implies D = \begin{pmatrix} k+1 & 0 \\ 0 & -1 \end{pmatrix}$$

9.7 Matrice di una trasformazione lineare

Definizione 106: Matrice di una trasformazione lineare

Siano V e W due spazi vettoriali e sia $f : V \rightarrow W$ una trasformazione lineare.

Data una base $\mathcal{B} = v_1, \dots, v_n$ di V , una base $\mathcal{C} = w_1, \dots, w_m$ di W e i seguenti due isomorfismi (sezione 8.3):

$$\varphi_{\mathcal{B}} : K^n \rightarrow V : (t_1, \dots, t_n) \mapsto (t_1 v_1 + \dots + t_n v_n)$$

$$\varphi_{\mathcal{C}} : K^m \rightarrow W : (s_1, \dots, s_m) \mapsto (s_1 w_1 + \dots + s_m w_m)$$

Definiamo come **matrice di f nelle basi \mathcal{B} e \mathcal{C}** l'unica matrice $M_f \in \text{Mat}_{m \times n}(K)$ tale che:

$$\exists! M_f \in \text{Mat}_{m \times n}(K) \mid f = \varphi_{\mathcal{C}} \circ L_{M_f} \circ \varphi_{\mathcal{B}}^{-1}$$

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ \varphi_{\mathcal{B}}^{-1} \downarrow & & \uparrow \varphi_{\mathcal{C}} \\ K^n & \xrightarrow{L_{M_f}} & K^m \end{array}$$

- Sia $L_A : K^n \rightarrow K^m$ una trasformazione lineare tale che:

$$f = \varphi_{\mathcal{C}} \circ L_A \circ \varphi_{\mathcal{B}}^{-1}$$

dove per definizione stessa di L_A è associata ad un'unica matrice $A \in \text{Mat}_{n \times m}(K)$

- Data la base canonica e_1, \dots, e_n di K^n , per ogni $i \in [1, n]$ si ha che:

$$\varphi_{\mathcal{B}}(e_i) = 0 \cdot v_1 + \dots + 1 \cdot v_i + \dots + 0 \cdot v_n = v_i \implies \varphi_{\mathcal{B}}^{-1}(v_i) = e_i$$

- Inoltre, per ogni $i \in [1, n]$ si ha che:

$$L_A(e_i) = Ae_i = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_{1,i} \\ \vdots \\ a_{m,i} \end{pmatrix} = A^i$$

- Infine, dato il seguente isomorfismo:

$$\varphi_{\mathcal{C}} : K^m \rightarrow W : (s_1, \dots, s_m) \mapsto (s_1 w_1 + \dots + s_m w_m)$$

per ogni $i \in [1, n]$ si ha che:

$$\varphi_{\mathcal{C}}(A^i) = a_{1,i}w_1 + \dots + a_{m,i}w_m$$

- A questo punto, per ogni $i \in [1, n]$ si ha che:

$$\begin{aligned} f(v_i) &= \varphi_{\mathcal{C}}(L_A(\varphi_{\mathcal{B}^{-1}}(v_i))) \iff \\ \iff f(v_i) &= \varphi_{\mathcal{C}}(L_A(e_i)) \iff f(v_i) = \varphi_{\mathcal{C}}(A^i) \iff \\ f(v_i) &= a_{1,i}w_1 + \dots + a_{m,i}w_m \end{aligned}$$

- Dunque, è possibile ricostruire la matrice A tramite le seguenti combinazioni lineari:

$$\begin{aligned} f(v_1) &= a_{1,1}w_1 + \dots + a_{m,1}w_m \implies A^1 = \begin{pmatrix} a_{1,1} \\ \vdots \\ a_{m,1} \end{pmatrix} \\ &\vdots \\ f(v_n) &= a_{1,n}w_1 + \dots + a_{m,n}w_m \implies A^n = \begin{pmatrix} a_{1,n} \\ \vdots \\ a_{m,n} \end{pmatrix} \end{aligned}$$

□

Esempi:

1. • Consideriamo i seguenti due sottospazi vettoriali di $\mathbb{R}[x]$:

$$V := \mathbb{R}[x]_{\leq 4} = \{p(x) \in \mathbb{R}[x] \mid \deg(p(x)) \leq 4\}$$

$$W := \mathbb{R}[x]_{\leq 3} = \{p(x) \in \mathbb{R}[x] \mid \deg(p(x)) \leq 3\}$$

dove $\mathcal{B} : x^4, x^3, x^2, x, 1$ è base di V e $\mathcal{C} : x^4, x^3, x^2, x, 1$ è base di W , da cui ne segue che:

$$\dim(V) = 5 = \dim(\mathbb{R}^5) \iff V \cong \mathbb{R}^5$$

$$\dim(W) = 4 = \dim(\mathbb{R}^4) \iff W \cong \mathbb{R}^4$$

- 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:

$$\begin{cases} f'(x^4) = 4x^3 = 4x^3 + 0x^2 + 0x + 0 \\ f'(x^3) = 3x^2 = 0x^3 + 3x^2 + 0x + 0 \\ f'(x^2) = 2x = 0x^3 + 0x^2 + 2x + 0 \\ f'(x) = x = 0x^3 + 0x^2 + 0x + 1 \\ f'(1) = 0 = 0x^3 + 0x^2 + 0x + 0 \end{cases} \implies M_{f'} = \begin{pmatrix} 4 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

- Consideriamo quindi i seguenti isomorfismi:

$$\varphi_{\mathcal{B}}^{-1} : V \rightarrow \mathbb{R}^5 : ax^4 + bx^3 + cx^2 + dx + e \mapsto \begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix}$$

$$\varphi_{\mathcal{C}} : \mathbb{R}^4 \rightarrow W : \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \mapsto ax^3 + bx^2 + cx + d$$

- Dato il polinomio $p(x) := 4x^4 + 2x^3 + x + 5 \in V$, si ha che:

$$\begin{aligned} \varphi_{\mathbb{B}}^{-1}(p(x)) = \begin{pmatrix} 4 \\ 2 \\ 0 \\ 1 \\ 5 \end{pmatrix} &\implies L_{M_f}(\varphi_{\mathcal{B}}^{-1}(p(x))) = \begin{pmatrix} 4 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 4 \\ 2 \\ 0 \\ 1 \\ 5 \end{pmatrix} = \begin{pmatrix} 16 \\ 6 \\ 0 \\ 1 \end{pmatrix} \\ &\implies \varphi_{\mathcal{C}} L_{M_f}(\varphi_{\mathcal{B}}^{-1}(p(x))) = 16x^3 + 6x^2 + 1 \end{aligned}$$

- Consideriamo ancora gli spazi $V = \mathbb{R}[x]_{\leq 4}$ e $W = \mathbb{R}[x]_{\leq 3}$.
 - Sia $\Delta : V \rightarrow W : p(x) \mapsto p(x+1) - p(x)$ la trasformazione lineare corrispondente all'operatore differenza (anche detta "derivata discreta")
 - La matrice di Δ nelle basi \mathcal{B} e \mathcal{C} corrisponde a:

$$\begin{cases} \Delta(x^4) = (x+1)^4 - x^4 = 4x^3 + 6x^2 + 4x + 1 \\ \Delta(x^3) = (x+1)^3 - x^3 = 3x^2 + 3x + 1 \\ \Delta(x^2) = (x+1)^2 - x^2 = 2x + 1 \\ \Delta(x) = (x+1) - x = 1 \\ \Delta(1) = (x+1)^0 - x^0 = 0 \end{cases} \implies M_{\Delta} = \begin{pmatrix} 4 & 0 & 0 & 0 & 0 \\ 6 & 3 & 0 & 0 & 0 \\ 4 & 3 & 2 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

- 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 inoltre

$$\mathcal{B} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \quad \mathcal{C} = \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \begin{pmatrix} -2 \\ 1 \end{pmatrix}$$

rispettivamente la base di $V = \mathbb{R}^2$ e di $W = \mathbb{R}^2$

- Consideriamo quindi la matrice M_f di f nelle basi \mathbb{B} e \mathbb{C}

$$M_f = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

- Le coordinate della colonna M_f^1 corrisponderanno a:

$$\begin{aligned} a \begin{pmatrix} 1 \\ 1 \end{pmatrix} + c \begin{pmatrix} -2 \\ 1 \end{pmatrix} &= f \begin{pmatrix} 1 \\ 1 \end{pmatrix} \Rightarrow a \begin{pmatrix} 1 \\ 1 \end{pmatrix} + c \begin{pmatrix} -2 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 3 \cdot 1 \\ 2 \cdot 1 + 4 \cdot 1 \end{pmatrix} \Rightarrow \\ &\Rightarrow a \begin{pmatrix} 1 \\ 1 \end{pmatrix} + c \begin{pmatrix} -2 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ 6 \end{pmatrix} \Rightarrow \begin{cases} a - 2c = 4 \\ 3a + 4c = 6 \end{cases} \Rightarrow \\ &\Rightarrow \left(\begin{array}{cc|c} 1 & -2 & 4 \\ 3 & 4 & 6 \end{array} \right) \xrightarrow{R_2 - 3R_1} \left(\begin{array}{cc|c} 1 & -2 & 4 \\ 0 & 10 & -6 \end{array} \right) \xrightarrow{\frac{1}{10}R_2} \left(\begin{array}{cc|c} 1 & -2 & 4 \\ 0 & 1 & -\frac{3}{5} \end{array} \right) \xrightarrow{R_1 - 2R_2} \\ &\xrightarrow{R_1 - 2R_2} \left(\begin{array}{cc|c} 1 & 0 & \frac{14}{5} \\ 0 & 1 & -\frac{3}{5} \end{array} \right) \Rightarrow \begin{cases} a = \frac{14}{5} \\ c = -\frac{3}{5} \end{cases} \end{aligned}$$

- Analogamente, le coordinate di M_f^2 saranno:

$$\begin{aligned} b \begin{pmatrix} 1 \\ 1 \end{pmatrix} + d \begin{pmatrix} -2 \\ 1 \end{pmatrix} &= f \begin{pmatrix} 1 \\ -1 \end{pmatrix} \Rightarrow b \begin{pmatrix} 1 \\ 1 \end{pmatrix} + d \begin{pmatrix} -2 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 + 3(-1) \\ 2 + 4(-1) \end{pmatrix} \Rightarrow \\ &\Rightarrow b \begin{pmatrix} 1 \\ 1 \end{pmatrix} + d \begin{pmatrix} -2 \\ 1 \end{pmatrix} = \begin{pmatrix} -2 \\ -2 \end{pmatrix} \Rightarrow \begin{cases} b - 2d = -2 \\ 3b + 4d = -2 \end{cases} \Rightarrow \\ &\Rightarrow \left(\begin{array}{cc|c} 1 & -2 & -2 \\ 3 & 4 & -2 \end{array} \right) \xrightarrow{R_2 + (-3)R_1} \left(\begin{array}{cc|c} 1 & -2 & -2 \\ 0 & 10 & 4 \end{array} \right) \xrightarrow{R_2 \cdot \frac{1}{10}} \left(\begin{array}{cc|c} 1 & -2 & -2 \\ 0 & 1 & \frac{2}{5} \end{array} \right) \\ &\xrightarrow{R_1 + (-2)R_2} \left(\begin{array}{cc|c} 1 & 0 & -\frac{6}{5} \\ 0 & 1 & \frac{2}{5} \end{array} \right) \Rightarrow \begin{cases} b = -\frac{6}{5} \\ d = \frac{2}{5} \end{cases} \end{aligned}$$

- Dunque, concludiamo la matrice di f nelle basi \mathcal{B} e \mathcal{C} sia:

$$M_f = \begin{pmatrix} \frac{14}{5} & -\frac{6}{5} \\ -\frac{3}{5} & \frac{2}{5} \end{pmatrix}$$

Proposizione 70: Matrice di cambiamento di base

Sia V uno spazio vettoriale e siano $\mathcal{B} = v_1, \dots, v_n$ e $\mathcal{C} = w_1, \dots, w_n$ due basi di V .

Dato il vettore $v \in V$ tale che:

$$v = a_1 v_1 + \dots + a_n v_n = b_1 w_1 + \dots + b_n w_n$$

e dati i suoi **vettori delle coordinate** in base \mathcal{B} e \mathcal{C} :

$$v_{\mathcal{B}} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \quad v_{\mathcal{C}} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

Definiamo come **matrice di cambiamento di base** l'unica matrice $M_{\mathcal{C}}^{\mathcal{B}} \in \text{Mat}_{n \times n}(K)$ tale che:

$$\exists! M_{\mathcal{C}}^{\mathcal{B}} \in \text{Mat}_{n \times n}(K) \mid M_{\mathcal{C}}^{\mathcal{B}} \cdot v_{\mathcal{B}} = v_{\mathcal{C}}$$

Dimostrazione:

- Consideriamo l'automorfismo $\text{id} : V \rightarrow V : v \mapsto v$ e consideriamo l'endomorfismo $L_A : K^n \rightarrow K^n$ tale che

$$\text{id} = \varphi_{\mathcal{C}} \circ L_A \circ \varphi_{\mathcal{B}}^{-1}$$

dove

$$\varphi_{\mathcal{B}} : K^n \rightarrow V : (t_1, \dots, t_n) \mapsto (t_1 v_1 + \dots + t_n v_n)$$

$$\varphi_{\mathcal{C}} : K^n \rightarrow V : (s_1, \dots, s_n) \mapsto (s_1 w_1 + \dots + s_n w_n)$$

- Le colonne della matrice A corrisponderanno a:

$$\begin{aligned} \text{id}(v_1) = a_{1,1} w_1 + \dots + a_{m,1} w_n &\implies v_1 = a_{1,1} w_1 + \dots + a_{m,1} w_n \implies A^1 = \begin{pmatrix} a_{1,1} \\ \vdots \\ a_{m,1} \end{pmatrix} \\ &\vdots \\ \text{id}(v_n) = a_{1,n} w_1 + \dots + a_{m,n} w_n &\implies v_n = a_{1,n} w_1 + \dots + a_{m,n} w_n \implies A^n = \begin{pmatrix} a_{1,n} \\ \vdots \\ a_{m,n} \end{pmatrix} \end{aligned}$$

- Dato un vettore $v \in V$, poiché l'automorfismo $\text{id} : V \rightarrow V : v \mapsto v$ ha alcun effetto primario, l'unico effetto secondario ottenuto applicando la matrice di id al vettore contenente le coordinate di v in base \mathcal{B} sarà quello di restituire le coordinate di v in base \mathcal{C}

□

Esempio:

- Consideriamo le seguenti due basi dello spazio \mathbb{R}^2

$$\mathcal{B} = \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix} \right) \quad \mathcal{C} = \left(\begin{pmatrix} 5 \\ 6 \end{pmatrix}, \begin{pmatrix} 7 \\ 8 \end{pmatrix} \right)$$

- Consideriamo la matrice del cambiamento dalla base \mathcal{B} alla base \mathcal{C} :

$$M_{\mathcal{C}}^{\mathcal{B}} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

- Le coordinate della matrice del cambiamento di base corrisponderanno a:

$$\begin{aligned} a \begin{pmatrix} 5 \\ 6 \end{pmatrix} + c \begin{pmatrix} 7 \\ 8 \end{pmatrix} &= \begin{pmatrix} 1 \\ 2 \end{pmatrix} \implies \begin{cases} 5a + 7c = 1 \\ 6a + 8c = 2 \end{cases} \implies \begin{cases} a = 3 \\ c = -2 \end{cases} \\ b \begin{pmatrix} 5 \\ 6 \end{pmatrix} + d \begin{pmatrix} 7 \\ 8 \end{pmatrix} &= \begin{pmatrix} 3 \\ 4 \end{pmatrix} \implies \begin{cases} 5b + 7d = 3 \\ 6b + 8d = 4 \end{cases} \implies \begin{cases} b = 2 \\ d = -1 \end{cases} \\ &\implies M_{\mathcal{C}}^{\mathcal{B}} = \begin{pmatrix} 3 & 2 \\ -2 & -1 \end{pmatrix} \end{aligned}$$

- Consideriamo quindi il seguente vettore e le sue coordinate in base \mathcal{B} :

$$\begin{aligned} \begin{pmatrix} -5 \\ -4 \end{pmatrix} &= x \begin{pmatrix} 1 \\ 2 \end{pmatrix} + y \begin{pmatrix} 3 \\ 4 \end{pmatrix} \implies \\ &\implies \begin{cases} x + 3y = -5 \\ 2x + 4y = -4 \end{cases} \implies \begin{cases} x = 4 \\ y = -3 \end{cases} \end{aligned}$$

- Le sue coordinate in base \mathcal{C} corrisponderanno a:

$$\begin{pmatrix} 3 & 2 \\ -2 & -1 \end{pmatrix} \begin{pmatrix} 4 \\ -3 \end{pmatrix} = \begin{pmatrix} 12 - 6 \\ -8 + 3 \end{pmatrix} = \begin{pmatrix} 6 \\ -5 \end{pmatrix}$$

- Difatti, notiamo che:

$$6 \begin{pmatrix} 5 \\ 6 \end{pmatrix} - 5 \begin{pmatrix} 7 \\ 8 \end{pmatrix} = \begin{pmatrix} -5 \\ -4 \end{pmatrix}$$

9.8 Matrici ortogonali

Definizione 107: Base ortogonale

Sia v_1, \dots, v_n una base di \mathbb{R}^n . Tale base viene detta **ortogonale** se i vettori sono tutti **ortogonali** tra loro, dunque se

$$v_i v_j = 0, \forall i \neq j$$

Definizione 108: Base ortonormale

Sia v_1, \dots, v_n una base di \mathbb{R}^n . Tale base è detta **ortonormale** se i vettori sono tutti **ortogonali** tra loro e sono **versori**, ossia aventi norma pari ad 1, dunque se:

$$v_i v_j = \delta_{ij} = \begin{cases} \|v_i\| = 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}$$

dove δ_{ij} viene detto **delta di Kroneker**.

Osservazione 70

Le basi ortonormali possono essere ottenute da dalla base canonica e_1, \dots, e_n attraverso **rotazioni** e **riflessioni**

Osservazione 71

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:

$$w = (w \cdot v_1) \cdot v_1 + \dots + (w \cdot v_n) \cdot v_n$$

Proposizione 71: Matrice ortogonale

Data una matrice $A \in \text{Mat}_{n \times n}(\mathbb{R})$, tale matrice viene detta **matrice ortogonale** se si verifica una delle seguenti condizioni equivalenti:

- $A \cdot A^T = A^T \cdot A = I_n \iff A \in GL(n, \mathbb{R}) \mid A^{-1} = A^T$
- Le colonne A^1, \dots, A^n sono base ortonormale di \mathbb{R}^n
- Le righe A_1, \dots, A_n sono base ortonormale di \mathbb{R}^n
- $L_A : \mathbb{R}^n \rightarrow \mathbb{R}^n$ è isometria, ossia non cambia la distanza tra i punti del piano

(*dimostrazione omessa*)

Definizione 109: Gruppo ortogonale

Dato il gruppo $(GL(n, \mathbb{R}), \cdot)$, definiamo $O(n) \leq GL(n, \mathbb{R})$ come **gruppo ortogonale**, dove

$$O(n) = \{A \in GL(n, \mathbb{R}) \mid A^{-1} = A^T\}$$

Dimostrazione:

- $I_n^{-1} = I_n = I_n^T \implies I_n \in O(n)$
- $A, B \in O(n) \implies A^{-1} = A^T, B^{-1} = B^T \implies (AB)^{-1} = B^{-1}A^{-1} = B^T A^T = (AB)^T \implies AB \in O(n)$
- $A \in O(n) \implies A^{-1} = A^T \implies (A^{-1})^{-1} = A = (A^T)^T \implies (A^{-1})^{-1} = (A^{-1})^T \implies A^{-1} \in O(n)$

□

Proposizione 72: Normalizzazione di un vettore

Dato uno spazio vettoriale V e un vettore $v \in V$, la **normalizzazione di v** corrisponde a:

$$w = \frac{v}{\|v\|}$$

Dimostrazione:

- Poiché la norma di v , ossia $\|v\|$, corrisponde alla lunghezza geometrica di v , si vede facilmente che il vettore w ottenuto corrisponde ad un vettore avente la stessa direzione di v ma norma pari ad 1

□

Proposizione 73: Proiezione di un vettore

Dato uno spazio vettoriale V e due vettori $v, w \in V$, la **proiezione di v su w** corrisponde a:

$$\text{proj}_w(v) = \frac{v \cdot w}{w \cdot w} w$$

Dimostrazione:

- Consideriamo la normalizzazione u del vettore w :

$$u = \frac{w}{\|w\|}$$

- Sia $x := \text{proj}_w(v)$ il vettore corrispondente alla proiezione di v su w . Per definizione stessa di proiezione su vettore, tale vettore avrà la stessa direzione del vettore w e

di conseguenza anche la stessa direzione del vettore u . Dunque, si ha che:

$$x = \|x\| \cdot u$$

- Consideriamo quindi l'angolo θ interno ai vettori v e x . Per definizione stessa di coseno, si ha che:

$$\cos(\theta) = \frac{\|x\|}{\|v\|}$$

- Poiché w ha la stessa direzione di x , l'angolo interno ai vettori v e w coincide con l'angolo θ . Come visto nella sezione 8.5, si ha che:

$$\cos(\theta) = \frac{v \cdot w}{\|v\| \|w\|}$$

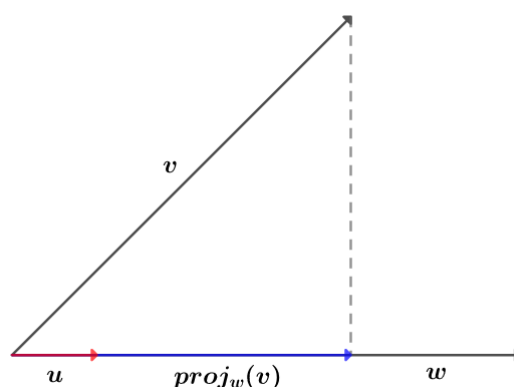
- Dunque, si ha che:

$$\frac{\|x\|}{\|v\|} = \cos(\theta) = \frac{v \cdot w}{\|v\| \|w\|} \implies \frac{\|x\|}{\|v\|} = \frac{v \cdot w}{\|w\|}$$

- Infine, concludiamo che:

$$x = \|x\| \cdot u = \frac{v \cdot w}{\|w\|} \cdot \frac{w}{\|w\|} = \frac{v \cdot w}{\|w\|^2} w = \frac{v \cdot w}{w \cdot w} w$$

- Di seguito, vi è un'interpretazione grafica dei passaggi effettuati:



□

Definizione 110: Matrice simmetrica

Data una matrice $A \in \text{Mat}_{n \times n}(K)$, tale matrice viene detta **simmetrica** se

$$A = A^T$$

Teorema 36: Teorema spettrale

Data una matrice simmetrica $S \in \text{Mat}_{n \times n}(\mathbb{R})$, le seguenti condizioni sono equivalenti:

1. $\text{sp}(S) \subset \mathbb{R}$
2. S è diagonalizzabile
3. Esiste una base ortonormale $\mathcal{B} = B^1, \dots, B^n$ di \mathbb{R}^n tale che $B^i, \forall i \in [1, n]$ è autovettore di S
4. $\exists B \in O(n) \mid D = B^{-1}AB = B^T AB$ dove $D \in \text{Mat}_{n \times n}(\mathbb{R})$ è una matrice diagonale

(dimostrazione omessa)

Algoritmo 2: Ortonormalizzazione di Gram-Schmidt

Sia V uno spazio vettoriale e sia v_1, \dots, v_n una sua base. Il seguente algoritmo restituisce una base ortogonale u_1, \dots, u_n di V e una base ortonormale w_1, \dots, w_n di V :

1. Poniamo $u_1 := v_1$
2. Il vettore u_2 corrisponderà a: $u_2 = v_2 - \text{proj}_{u_1}(v_2)$
3. Difatti, notiamo che:

$$\begin{aligned} u_1 \cdot u_2 &= u_1(v_2 - \text{proj}_{u_1}(v_2)) = u_1 \left(v_2 - \frac{u_1 \cdot v_2}{u_1 \cdot u_1} u_1 \right) u_1 = \\ &= u_1 v_2 - \frac{u_1 \cdot v_2}{\|u_1\|^2} \|u_1\|^2 = u_1 v_2 - u_1 v_2 = 0 \end{aligned}$$

dunque u_1 risulta essere ortogonale a u_2

4. In generale, il vettore u_k , dove $k \in [1, n]$, corrisponderà a:

$$u_k = v_k - \sum_{i=1}^{k-1} \text{proj}_{u_i}(v_k)$$

5. I vettori u_1, \dots, u_k costituiscono una base ortogonale di V .
6. Per ottenere la base ortonormale w_1, \dots, w_n , basterà normalizzare ogni vettore della base ortogonale:

$$w_k = \frac{u_k}{\|u_k\|}, \forall k \in [1, n]$$

10

Algoritmi di crittografia

10.1 Algoritmo RSA

Algoritmo 3: Algoritmo di crittografia RSA

Siano:

- $p, q \in \mathbb{P} \mid p \neq q$ e sufficientemente grandi
- $n := pq$
- $\lambda(n) := \text{mcm}(p-1, q-1)$
- $e \in \mathbb{N} \mid 1 < e < \lambda(n) \wedge \text{MCD}(e, \lambda(n)) = 1$
- $d := e^{-1}(\text{mod } \lambda(n))$

Dato un **messaggio da cifrare** m tale che $\text{MCD}(m, n) = 1$, il **messaggio cifrato** c ottenuto tramite la **chiave pubblica** (e, n) corrisponde a:

$$m^e \equiv c(\text{mod } n)$$

Una volta ottenuto il messaggio cifrato, applicando la **chiave privata** (d, n) è possibile riottenere il messaggio m :

$$c^d \equiv m(\text{mod } n)$$

Poiché le due chiavi sono **l'una l'inversa dell'altra**, distribuendo la propria chiave pubblica (e, n) è possibile permettere ad un interlocutore di poterci inviare messaggi cifrati, per poi decifrarli tramite la propria chiave privata (d, n) , la quale dovrà essere mantenuta **nascosta** al fine di non concedere ad altre persone di poter leggere il contenuto del messaggio m .

Dimostrazione:

- Poiché $\lambda(n) := \text{mcm}(p, q)$, si ha che:

$$\begin{cases} (p-1) \mid \lambda(n) \implies \exists k \in \mathbb{Z} \mid \lambda(n) = (p-1)k \\ (q-1) \mid \lambda(n) \implies \exists h \in \mathbb{Z} \mid \lambda(n) = (q-1)h \end{cases}$$

- Per il piccolo teorema di Fermat si ha che:

$$\begin{aligned} m^p &\equiv m \pmod{p} \iff m^{p-1} \equiv 1 \pmod{p} \implies \\ \implies m^{(p-1)k} &\equiv 1 \pmod{p} \iff m^{\lambda(n)} \equiv m \pmod{p} \end{aligned}$$

e analogamente:

$$\begin{aligned} m^q &\equiv m \pmod{q} \iff m^{q-1} \equiv 1 \pmod{q} \implies \\ \implies m^{(q-1)h} &\equiv 1 \pmod{q} \iff m^{\lambda(n)} \equiv m \pmod{q} \end{aligned}$$

- Poiché $\text{MCD}(p, q) = 1$, per il teorema cinese dei resti si ha che:

$$m^{\lambda(n)} \equiv 1 \pmod{p} m^{\lambda(n)} \equiv 1 \pmod{q} \iff m^{\lambda(n)} \equiv 1 \pmod{n}$$

- Inoltre, si ha che:

$$\begin{aligned} \text{MCD}(e, \lambda(n)) = 1 &\iff [e] \in \mathbb{Z}_{\lambda(n)}^* \iff \exists [d] := [e]^{-1} \in \mathbb{Z}_{\lambda(n)}^* \iff \\ &\iff ed \equiv 1 \pmod{\lambda(n)} \iff ed = 1 + b\lambda(n), \exists b \in \mathbb{Z} \end{aligned}$$

- Dunque, concludiamo che:

$$(m^e)^d \equiv m^{ed} \equiv m^{1+\lambda(n)b} \equiv m(m^{\lambda(n)})^b \equiv m(1)^b \equiv m \pmod{n}$$

□

Osservazione 72

La condizione $\text{MCD}(m, n) = 1$ è **necessaria** affinché non vi sia una **perdita del messaggio** durante il processo di cifratura e de-cifratura. Difatti, tramite tale condizione si ha che:

$$\text{MCD}(m, n) = 1 \implies \begin{cases} n \nmid m \iff \nexists k \in \mathbb{Z} \mid m = nk \iff m \not\equiv 0 \pmod{n} \\ p \nmid m \iff \nexists h \in \mathbb{Z} \mid m = ph \iff m \not\equiv 0 \pmod{p} \\ q \nmid m \iff \nexists b \in \mathbb{Z} \mid m = qb \iff m \not\equiv 0 \pmod{q} \end{cases}$$

Senza tale condizione, quindi, potrebbe verificarsi che $n \mid m \vee p \mid m \vee q \mid m$, portando ad una perdita del messaggio.

Osservazione 73

I due primi $p, q \in \mathbb{P}$ devono essere **sufficientemente grandi** poiché altrimenti sarebbe possibile ricavare gli interi componenti dell'algoritmo tramite essi, ottenendo quindi anche la **chiave privata** (d, n) .

Difatti, poiché l'intero $n := pq$ è contenuto nella chiave pubblica (e, n) , se p o q fossero due numeri piccoli si potrebbe ricavare l'uno dall'altro procedendo per **brute-force**:

1. Preso $k \in \mathbb{P}$, se $k \mid n$ allora $k = p$ e $q = \frac{n}{k}$
2. Se invece $k \nmid n$, allora verrà ripetuto il passo precedente con il numero primo successivo
3. Una volta trovati p e q , basterà calcolare $[d] := [e]^{-1}(\bmod \lambda(n))$ per poter ottenere la chiave privata (d, n)

10.2 Interpolazione di Lagrange e Algoritmo SSS

Definizione 111: Matrice di Vandermonde

Dati $x_0, \dots, x_n \in K$, definiamo la seguente matrice $V \in \text{Mat}_{n \times n}(K)$ come **matrice di Vandermonde a coefficienti** x_0, \dots, x_n :

$$V(x_0, x_1, \dots, x_n) = \begin{pmatrix} x_0^0 & x_0^1 & x_0^2 & \cdots & x_0^n \\ x_1^0 & x_1^1 & x_1^2 & \cdots & x_1^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_n^0 & x_n^1 & x_n^2 & \cdots & x_n^n \end{pmatrix}$$

Proposizione 74

Dati $x_0, \dots, x_n \in K$, si ha che:

$$\det(V(x_0, \dots, x_n)) = \prod_{0 \leq i < j \leq n} (x_j - x_i)$$

Dimostrazione:

- Consideriamo il determinante di $V(x_0, \dots, x_n)$:

$$\det(V(x_0, x_1, \dots, x_n)) = \det \begin{pmatrix} x_0^0 & x_0^1 & x_0^2 & \cdots & x_0^n \\ x_1^0 & x_1^1 & x_1^2 & \cdots & x_1^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_n^0 & x_n^1 & x_n^2 & \cdots & x_n^n \end{pmatrix} = \det \begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^n \\ 1 & x_1 & x_1^2 & \cdots & x_1^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^n \end{pmatrix}$$

- Poiché sottrarre un multiplo di una riga non ha effetti sul determinante, sottraendo la prima riga a tutte le altre si ha che:

$$\det \begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^n \\ 1 & x_1 & x_1^2 & \cdots & x_1^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^n \end{pmatrix} \xrightarrow{R_i - R_1, \forall i > 1} \det \begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^n \\ 0 & x_1 - x_0 & x_1^2 - x_0^2 & \cdots & x_1^n - x_0^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & x_n - x_0 & x_n^2 - x_0^2 & \cdots & x_n^n - x_0^n \end{pmatrix}$$

- Eseguendo lo sviluppo di Laplace sulla prima colonna, si ha che:

$$\det \begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^n \\ 0 & x_1 - x_0 & x_1^2 - x_0^2 & \cdots & x_1^n - x_0^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & x_n - x_0 & x_n^2 - x_0^2 & \cdots & x_n^n - x_0^n \end{pmatrix} = 1 \cdot \det \begin{pmatrix} x_1 - x_0 & x_1^2 - x_0^2 & \cdots & x_1^n - x_0^n \\ \vdots & \vdots & \ddots & \vdots \\ x_n - x_0 & x_n^2 - x_0^2 & \cdots & x_n^n - x_0^n \end{pmatrix}$$

- Notiamo che $\forall i, k \in [1, n]$ si ha che:

$$x_i^k - x_0^k = (x_i - x_0)(x_i^{k-1} + x_i^{k-2}x_0 + \dots + x_i x_0^{k-2} + x_0^{k-1})$$

da cui ne segue che:

$$\begin{aligned} & \det \begin{pmatrix} x_1 - x_0 & x_1^2 - x_0^2 & \cdots & x_1^n - x_0^n \\ \vdots & \vdots & \ddots & \vdots \\ x_n - x_0 & x_n^2 - x_0^2 & \cdots & x_n^n - x_0^n \end{pmatrix} = \\ & = \det \begin{pmatrix} x_0 & x_0^2 & \cdots & x_0^n \\ x_1 - x_0 & (x_1 - x_0)(x_1 + x_0) & \cdots & (x_1 - x_0)(x_1^{n-1} + x_1^{n-2}x_0 + \dots + x_1 x_0^{n-2} + x_0^{n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ x_n - x_0 & (x_n - x_0)(x_n + x_0) & \cdots & (x_n - x_0)(x_n^{n-1} + x_n^{n-2}x_0 + \dots + x_n x_0^{n-2} + x_0^{n-1}) \end{pmatrix} \end{aligned}$$

- Per multilinearit  del determinante, si ha che:

$$\begin{aligned} & \det \begin{pmatrix} x_1 - x_0 & (x_1 - x_0)(x_1 + x_0) & \cdots & (x_1 - x_0)(x_1^{n-1} + x_1^{n-2}x_0 + \dots + x_1 x_0^{n-2} + x_0^{n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ x_n - x_0 & (x_n - x_0)(x_n + x_0) & \cdots & (x_n - x_0)(x_n^{n-1} + x_n^{n-2}x_0 + \dots + x_n x_0^{n-2} + x_0^{n-1}) \end{pmatrix} = \\ & (x_1 - x_0) \cdots (x_n - x_0) \cdot \det \begin{pmatrix} 1 & x_1 + x_0 & \cdots & x_1^{n-1} + x_1^{n-2}x_0 + \dots + x_1 x_0^{n-2} + x_0^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n + x_0 & \cdots & x_n^{n-1} + x_n^{n-2}x_0 + \dots + x_n x_0^{n-2} + x_0^{n-1} \end{pmatrix} = \\ & = \prod_{j=1}^n (x_j - x_0) \cdot \det \begin{pmatrix} 1 & x_1 + x_0 & \cdots & x_1^{n-1} + x_1^{n-2}x_0 + \dots + x_1 x_0^{n-2} + x_0^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n + x_0 & \cdots & x_n^{n-1} + x_n^{n-2}x_0 + \dots + x_n x_0^{n-2} + x_0^{n-1} \end{pmatrix} \end{aligned}$$

- Sottraendo ad ogni colonna tutte le colonne precedenti moltiplicate per b_0 , si ha che:

$$\prod_{j=1}^n (x_j - x_0) \cdot \det \begin{pmatrix} 1 & x_1 + x_0 & \cdots & x_1^{n-1} + x_1^{n-2}x_0 + \cdots + x_1x_0^{n-2} + x_0^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n + x_0 & \cdots & x_n^{n-1} + x_n^{n-2}x_0 + \cdots + x_nx_0^{n-2} + x_0^{n-1} \end{pmatrix} \xrightarrow{C^i - \sum_{j=1}^{n-1} x_0 C^j, \forall i}$$

$$\prod_{j=1}^n (x_j - x_0) \cdot \det \begin{pmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \cdots & x_n^{n-1} \end{pmatrix} = \prod_{j=1}^n (x_j - x_0) \cdot \det(V(x_1, \dots, x_n))$$

- Effettuando gli stessi passaggi ricorsivamente, concludiamo che:

$$\det(V(x_0, \dots, x_n)) = \prod_{j=1}^n (x_j - x_0) \cdot \det(V(x_1, \dots, x_n)) =$$

$$= \prod_{j=1}^n (x_j - x_0) \cdot \prod_{h=2}^n (x_h - x_1) \cdot \det(V(x_2, \dots, x_n)) = \dots = \prod_{0 \leq i < j \leq n} (x_j - x_i)$$

□

Lemma 21

Dati $x_0, \dots, x_n \in K$, si ha che:

$$\det(V(x_0, \dots, x_n)) \neq 0 \iff x_i \neq x_j, \forall i \neq j$$

Dimostrazione:

- Poiché

$$\det(V(x_0, \dots, x_n)) = \prod_{0 \leq h < j \leq n} (x_j - x_h)$$

si vede facilmente che:

$$\exists k, h \in [0, n] \mid x_k = x_h \implies x_k - x_h = 0 \implies \det(V(x_0, \dots, x_n)) = 0$$

da cui per contronominale otteniamo che:

$$\det(V(x_0, \dots, x_n)) \neq 0 \implies \nexists k, h \in [0, n] \mid x_k = x_h \implies x_k \neq x_h, \forall k, h \in [0, n]$$

- Viceversa, supponiamo per assurdo che $x_i \neq x_j, \forall i \neq j$ e che $\det(V(x_0, \dots, x_n)) = 0$. Ne segue che:

$$\det(V(x_0, \dots, x_n)) = 0 \iff \prod_{0 \leq i < j \leq n} (x_j - x_i) = 0$$

- Per la legge di annullamento del prodotto, ne segue che:

$$\prod_{0 \leq i < j \leq n} (x_j - x_i) = 0 \implies (x_1 - x_0) = 0 \vee \dots \vee (x_n - x_{n-1}) = 0 \implies$$

$$x_1 = x_0 \vee \dots \vee x_n = x_{n-1}$$

contraddicendo quindi l'ipotesi per cui $x_k \neq x_j, \forall i \neq j$. Dunque, l'unica possibilità è che $\det(V(x_0, \dots, x_n)) \neq 0$

□

Proposizione 75

Siano $x_0, \dots, x_n \in K \mid x_i \neq x_j, \forall i \neq j$. Dati $y_0, \dots, y_n \in K$, si ha che:

$$\exists! p(x) \in K[x]_{\leq n} \mid \begin{cases} p(x_0) = y_0 \\ \vdots \\ p(x_n) = y_n \end{cases}$$

Dimostrazione:

- Posto $p(x) := a_0 + a_1x + \dots + a_nx^n \in K[x]_{\leq n}$, si ha che:

$$\begin{cases} p(x_0) = y_0 \\ \vdots \\ p(x_n) = y_n \end{cases} \iff \begin{cases} a_0 + a_1x_0 + \dots + a_nx_0^n = y_0 \\ \vdots \\ a_0 + a_1x_n + \dots + a_nx_n^n = y_n \end{cases}$$

- Considerando a_0, \dots, a_n come le incognite del sistema, la matrice dei coefficienti associata a risulta essere una matrice di Vandermonde nella forma $V(x_0, \dots, x_n)$. Di conseguenza, si ha che:

$$x_i \neq x_j, \forall i \neq j \iff \det(V(x_0, \dots, x_n)) \neq 0 \iff \exists! \text{ soluzione}$$

- Dunque, esiste può esistere un'unico polinomio $p(x) \in K_{\leq n} \mid p(x_0) = y_0, \dots, p(x_n) = y_n$

□

Corollario 33

Dati $x_0, \dots, x_n \in K \mid x_i \neq x_j, \forall i \neq j$, si ha che:

$$\exists! p_i(x) \in K[x]_{\leq n} \mid p_i(x_j) = \delta_{i,j} = \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}$$

dove $\delta_{i,j}$ è il **delta di Kroneker** e dove p_1, \dots, p_n formano una base di $K[x]_{\leq n}$ detta **base di Lagrange**

Dimostrazione:

- Dato $i \in [0, n]$, si ha che:

$$p_i(x_j) = \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases} \iff (x - x_j) \mid p_i(x), \forall j \neq i \in [0, n] \iff \begin{cases} p_i(x_1) = 0 \\ \vdots \\ p_i(x_i) = 1 \\ \vdots \\ p_i(x_n) = 0 \end{cases}$$

- Per la proposizione precedente, l'unica possibilità è che $p_0(x), \dots, p_n(x) \in K[x]_{\leq n}$ siano unici, poiché:

$$\exists! q(x) \in K[x]_{\leq n} \mid q(x_1) = 0, \dots, q(x_i) = 1, \dots, q(x_n) = 0$$

□

- Di conseguenza, ne segue automaticamente che tali polinomi siano linearmente indipendenti tra loro, poiché nessuno di loro può essere espresso come combinazione lineare degli altri.
- Inoltre, poiché $\dim(K[x]_{\leq n}) = n + 1$, sappiamo che $n + 1$ vettori possono essere linearmente indipendenti se e solo se sono anche generatori, di conseguenza p_0, \dots, p_n sono una base di $K[x]_{\leq n}$

□

Teorema 37: Interpolazione di Lagrange

Dati i seguenti **nodì dell'interpolazione** $(x_0, y_0), \dots, (x_n, y_n)$, dove $x_i \neq x_j, \forall i \neq j$, e dati i seguenti polinomi $p_0, \dots, p_n \in K[x]_{\leq n}$ tali che:

$$p_i(x) = \prod_{0 \leq j \leq n, j \neq i} \frac{x - x_j}{x_i - x_j}$$

L'unico polinomio $p(x) \in K[x]_{\leq n}$ passante per ogni nodo corrisponde a:

$$p(x) = y_0 p_0(x) + \dots + y_n p_n(x)$$

Dimostrazione:

- Consideriamo la base di Lagrange $p_0, \dots, p_n \in K[x]_{\leq n}$ dello spazio $K[x]_{\leq n}$ vista nel corollario precedente:

$$\exists! p_i(x) \in K[x]_{\leq n} \mid p_i(x_j) = \delta_{i,j} = \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}$$

- Per ogni polinomio della base si ha che:

$$p_i(x_j) = 0, \forall j \neq i \in [0, n] \iff (x - x_j) \mid p_i(x), \forall j \neq i \in [0, n] \implies$$

$$\begin{aligned} &\implies (x - x_1) \cdot \dots \cdot (x - x_{i-1})(x - x_{i+1}) \cdot \dots \cdot (x - x_n) \mid p_i(x) \iff \\ &\iff p_i(x) = c_i(x - x_1) \cdot \dots \cdot (x - x_{i-1})(x - x_{i+1}) \cdot \dots \cdot (x - x_n), \exists c_i \in K \end{aligned}$$

- Poiché $p_i(x_i) = 1, \forall i \in [0, n]$, l'unica possibilità è che $c_i = 1, \forall i \in [0, n]$. Inoltre, poiché $p_i(x_i) = 1$, ne segue che:

$$\begin{aligned} p_i(x) &= (x - x_1) \cdot \dots \cdot (x - x_{i-1})(x - x_{i+1}) \cdot \dots \cdot (x - x_n) \implies \\ p_i(x) &= \frac{(x - x_1) \cdot \dots \cdot (x - x_{i-1})(x - x_{i+1}) \cdot \dots \cdot (x - x_n)}{1} \implies \\ p_i(x) &= \frac{(x - x_1) \cdot \dots \cdot (x - x_{i-1})(x - x_{i+1}) \cdot \dots \cdot (x - x_n)}{p_i(x_i)} \implies \\ p_i(x) &= \frac{(x - x_1) \cdot \dots \cdot (x - x_{i-1})(x - x_{i+1}) \cdot \dots \cdot (x - x_n)}{(x_i - x_1) \cdot \dots \cdot (x_i - x_{i-1})(x_i - x_{i+1}) \cdot \dots \cdot (x_i - x_n)} = \\ p_i(x) &= \prod_{0 \leq j \leq n, j \neq i} \frac{x - x_j}{x_i - x_j} \end{aligned}$$

- Sia quindi $p(x) \in K[x]_{\leq n}$ definito come:

$$p(x) := y_0 p_0(x) + \dots + y_n p_n(x)$$

- Dunque, $\forall k \in [0, n]$ si ha che:

$$\begin{aligned} p(x_k) &= y_0 p_0(x_k) + \dots + y_k p_k(x_k) + \dots + y_n p_n(x_k) \implies \\ p(x_k) &= y_0 \cdot 0 + \dots + y_k \cdot 1 + \dots + y_n \cdot 0 = y_k \implies \begin{cases} p(x_0) = y_0 \\ \vdots \\ p(x_n) = y_n \end{cases} \end{aligned}$$

- Per la proposizione precedente, concludiamo che $p(x)$ sia l'unico polinomio in $K[x]_{\leq n}$ tale che $p(x_0) = y_0, \dots, p(x_n) = y_n$

□

Osservazione 74

Dati $n + 1$ punti del piano cartesiano $(x_0, y_0), \dots, (x_n, y_n)$, è possibile utilizzare l'interpolazione di Lagrange per trovare l'unico polinomio di grado n , dunque $p(x) \in K[x]_{\leq n}$, passante per ognuno di tali punti

Algoritmo 4: Algoritmo SSS

Il seguente algoritmo permette di suddividere in $n + 1$ **partizioni** un **segreto** $s \in K$, per poi ricostruire il quest'ultimo tramite le partizioni stesse:

1. Scelti casualmente i coefficienti $a_1, \dots, a_n \in K$, definiamo $p(x) \in K[x]_{\leq n}$ come:

$$p(x) = s + a_1x + \dots + a_nx_n$$

2. Scelti $n + 1$ valori $x_0, \dots, x_n \mid x_i \neq x_j, \forall i \neq j$, costruiamo i nodi dell' **interpolazione di Lagrange** come $(x_0, p(x_0)), \dots, (x_n, p(x_n))$
3. Distribuiamo ogni nodo ad eventuali interlocutori
4. Una volta riottenuti gli $n + 1$ nodi, tramite l'interpolazione di Lagrange è possibile ricostruire $p(x)$
5. Infine, poiché s è il termine noto di $p(x)$, è possibile riottenere il segreto tramite $p(0) = s$