SAPIENZA
UNIVERSITÀ DI ROMA

UNIVERSITÀ "SAPIENZA" DI ROMA
FACOLTÀ DI INFORMATICA

Algebra

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

Author
Simone Bianco

24 novembre 2022

Indice

Capitolo 0

Introduzione

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

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

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

Capitolo 1

Strutture algebriche principali

1.1 Richiami di insiemistica

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

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

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

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

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

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

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

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

$$A \subseteq S \iff x \in A \implies x \in X$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$\texttt{Suriettività} : Im(f) = Y$$

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

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

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

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

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

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

- Definiamo come **insieme dei numeri naturali** l'insieme

$$\mathbb{N} : \{0, 1, 2, 3, \ldots\}$$

- Definiamo come **insieme dei numeri interi** l'insieme

$$\mathbb{Z} : \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

- Definiamo come **insieme dei numeri razionali** l'insieme

$$\mathbb{Q} : \left\{\frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0\right\}$$

- Definiamo come **insieme dei numeri irrazionali** l'insieme

$$\mathbb{I} : \left\{x \mid \nexists m, n \in \mathbb{Z} : x = \frac{m}{n}\right\}$$

- Definiamo come **insieme dei numeri reali** l'insieme

$$\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$$

1.2 Operazioni binarie, Assiomi e Proprietà

Una particolare categoria di funzioni che studieremo durante il corso corrisponde alle **operazioni binarie**:

Definition 1. Operazione binaria

Dato un insieme S, definiamo **operazione binaria** una funzione che manda ogni coppia di elementi appartenenti ad S in S stesso. Tale proprietà viene anche detta **assioma di chiusura**.

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

Ad esempio, sull'insieme $\mathbb{R}$ possiamo considerare l'**operazione binaria additiva**, indicata come

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

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

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

Inoltre, anche la **composizione tra funzioni** corrisponde ad un'operazione binaria:

$$\circ : X \times X \to X : (g, f) \to g \circ f$$

Definition 2. Associatività (Assioma 1)

Data un'operazione binaria $m : S \times S \to S$ e tre elementi $x, y, z \in S$, l'**ordine di applicazione** di tale operazione binaria non influenza il risultato

$$m(m(x, y), z) = m(x, m(y, z)) \quad \forall x, y, z \in S$$

Esempi:

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

Definition 3. Elemento neutro (Assioma 2)

Data un'operazione binaria $m : S \times S \to S$, esiste un **elemento neutro** e tale che

$$m(x, e) = m(e, x) = x \quad \forall x \in S$$

Esempi:

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

Definition 4. Elemento inverso (Assioma 3)

Data un'operazione binaria $m : S \times S \to S$, per ogni elemento $x \in S$, esiste un **elemento inverso** x^{-1} tale che

$$m(x, x^{-1}) = m(x^{-1}, x) = e$$

Attenzione: con x^{-1} indichiamo l'inverso di x rispetto all'operazione, non necessariamente l'inverso moltiplicativo "classico" (ossia $\frac{1}{x}$)

Esempi:

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

Definition 5. Commutatività (Assioma 4)

Data un'operazione binaria $m : S \times S \to S$, l'ordine elementi non influenza il risultato

$$m(x, y) = m(y, x) \quad \forall x \in S$$

Esempi:

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

Observation 1

1. Può esistere **un solo elemento neutro**:

$$e_1 = m(e_1, e_2) = m(e_2, e_1) = e_2 \implies e_1 = e_2$$

2. Può esistere **un solo elemento inverso**:

$$m(x, x_1^{-1}) = e = m(x, x_2^{-1}) \implies m(x, x_1^{-1}) = m(x, x_2^{-1}) \implies x_1^{-1} = x_2^{-1}$$

1.3 Semigruppi, Monoidi e Gruppi

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

Definition 6. Strutture algebriche semplici

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

- Un **semigruppo** se vale l'assioma di associatività (assioma 1)
- Un **monoide** se valgono gli assiomi di d'associatività e di elemento neutro (assiomi 1 e 2)
- Un **gruppo** se valgono gli assiomi di associatività, elemento neutro e elemento inverso (assiomi 1, 2 e 3)
- Un **gruppo abeliano** (o commutativo) se valgono gli assiomi di associatività, elemento neutro, elemento inverso e commutatività (assiomi 1, 2, 3 e 4)

Esempi:

- $(\mathbb{N} - \{0\}, +)$ è un **semigruppo** (assioma 1)
- $(\mathbb{N}, +)$ è un **monoide** commutativo (assiomi 1, 2 e 4)
- $(\mathbb{Q}, \div)$ è un **gruppo** (assiomi 1, 2, 3 e 4)
- $(\mathbb{Z}, \cdot)$ è un **monoide** commutativo (assiomi 1, 2 e 4)
- Dati due insiemi X, Y, denotiamo con Y^X l'insieme composto da tutte le funzioni da X in Y

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

  Allora, la coppia $(X^X, \circ)$ è un monoide, poiché si ha:
  - **Associatività**: $f, g, h : X \to X \implies h \circ (g \circ f) = (h \circ g) \circ f$
  - **Elemento neutro**: $\exists \texttt{id} \in X^X \mid \forall f \in X^X, f \circ \texttt{id} = \texttt{id} \circ f = f$ dove `id` è la funzione identità, ossia $id(x) = x$.

1.4 Anelli e Campi

Consideriamo un insieme A e le due operazioni di somma e prodotto, definite come:

$$+ : A \times A \to A$$

$$\cdot : A \times A \to A$$

Se tale struttura algebrica risulta essere un **gruppo abeliano** nell'operazione somma, un **monoide** nell'operazione prodotto e vale la **relazione distributiva** tra le due operazioni, allora definiamo tale struttura algebrica come **anello**.

Definition 7. Anello

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

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

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

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

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

Observation 2

In un anello $(A, +, \cdot)$ applicare l'operazione prodotto tra un qualsiasi elemento $a \in A$ e l'elemento neutro 0 dell'operazione somma, restituirà l'elemento neutro 0 come risultato:

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

Dimostrazione:

- Riscriviamo l'elemento $a \in A$ come:

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

- A questo punto, abbiamo che:

$$a = a \cdot 0 + a$$

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

$$0 = a \cdot 0$$

Se un anello commutativo A ammette anche l'assioma di elemento inverso per il prodotto, allora viene definito come campo:

Definition 8. Campo

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

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

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

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

Esempi:

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

1.5 Sottogruppi ed Ideali

Definition 9. Sottogruppo

Sia $(G, \cdot)$ un gruppo. Definiamo $H \subseteq G$ come **sottogruppo** di G se:

- $e \in G \implies e \in H$
- $x, y \in H \implies xy \in H$
- $x \in H \implies x^{-1} \in H$

Esempi:

- $(\mathbb{Z}, +) \subseteq (\mathbb{Q}, +) \subseteq (\mathbb{R}, +) \subseteq (\mathbb{C}, +)$
- $(\mathbb{Z} \setminus \{0\}, \cdot) \not\subseteq (\mathbb{Q} \setminus \{0\}, \cdot) \subseteq (\mathbb{R} \setminus \{0\}, \cdot)$
- Sia A un anello. Dato $a \in A$, definiamo $I(a) : \{I(a) : \{ax \mid x \in A\}\}$, ossia l'insieme dei multipli di a in A. Dimostriamo quindi che $I(a) \subseteq A$ è sottogruppo:
  - $0 = a \cdot 0$, dunque $0 \in I(a)$
  - $x, y \in I(a) \implies \exists b, c \in A \mid x = ab, y = ac \implies x + y = ab + ac = a(b + c) \implies x + y \in I(a)$
  - $x \in I(a) \implies \exists b \in A \mid x = ab \implies -x = a(-b) \implies -x \in I(a)$

Definition 10. Ideale

Definiamo $I \subseteq A$ come **ideale** di A, dove $(A, +, \cdot)$ è un **anello commutativo**, se si verifica che:

- $(I, +) \subseteq (A, +)$ è sottogruppo
- $x \in I, a \in A \implies ax = xa \in I$ ossia se $AI = IA \subseteq I$, dove $AI : \{ax \mid x \in I, a \in A\}$ e $IA : \{xa \mid x \in I, a \in A\}$

Esempi:

- Sia $a \in A$, dove A è un anello commutativo e sia $I(a) : \{ak \mid k \in Z\}$. In tal caso, definiamo $I(a) \subseteq A$ come l'**ideale principale di A generato da a**.

  Verifica delle condizioni per l'ideale:

  - Abbiamo già verificato precedentemente che $(I(a), +) \subseteq (A, +)$
  - Sappiamo già che $a \in A$, dunque verifichiamo che:

    $$x \in I(a) \implies \exists c \in A, x = ac \implies b \in A \mid bx = bac = a(bc) \implies bx \in I(a)$$

- Siano $a_1, a_2 \in A$, dove A è un anello commutativo, e sia $I(a_1, a_2) : \{a_1b_1 + a_2b_2 \mid b_1, b_2 \in A\}$. Verifichiamo che $I(a_1, a_2) \subseteq A$ è ancora un ideale di A, che denotiamo come **ideale di A generato da a e b**:

  Verifica delle condizioni per l'ideale:

  - $0 = a_1 \cdot 0 + a_2 \cdot 0 \in I(a_1, a_2)$
  - $x, y \in I(a_1, a_2) \implies x = a_1b_1 + a_2b_2, y = a_1c_1 + a_2c_2 \implies x + y = a_1(b_1 + c_1) + a_2(b_2 + c_2) \implies x + y \in I(a_1, a_2)$
  - $x \in I(a_1, a_2) \implies x = a_1b_1 + a_2 + b_2 \implies -x = -a_1b_1 + a_2b_2 = a_1(-b_1) + a_2(-b_2) \implies -x \in I(a_1, a_2)$
  - $x \in I(a_1, a_2) \implies x = a_1b_1 + a_2b_2 \implies c \in A \mid cx = c(a_1b_1 + a_2b_2) = a_1(b_1c) + a_2(b_2c) \implies cx \in I(a_1, a_2)$

- Analogamente ai due casi precedenti, possiamo verificare che, **più genericamente**, anche $I(a_1, \ldots, a_n) : \{a_nb_1 + \ldots + a_nb_n \mid b_j \in A\}$ risulta essere un'ideale di A.

Definition 11. Somma tra ideali

Dati due ideali $I, J \subseteq A$, definiamo la loro somma come:

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

Dimostrazione:

- $I + J$ è sottogruppo di A, poiché:
  - $0 \in I \land 0 \in J \implies 0 = 0 + 0 \in I + J$
  - $x, y \in I + J \implies x + y = (i_1 + j_1) + (i_2 + j_2) = (i_1 + i_2) + (j_1 + j_2) \in I + J$
  - $x = i + j \in I + J \implies -x = -(i + y) = (-i) + (-j), -i \in I, -j \in J \implies -x \in I + J$
- $a \in A, x \in I + J \implies ax \in I + J$, poiché:

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

Definition 12. Intersezione tra ideali

Dati due ideali $I, J \subseteq A$, definiamo la loro intersezione come:

$$I \cap J \subseteq A : \{i \mid i \in I \land i \in J\}$$

Dimostrazione:

- $I \cap J$ è sottogruppo di A, poiché:
  - $0 \in I \land 0 \in J \implies 0 \in I \cap J$
  - $x, y \in I \cap J \implies x, y \in I \land x, y \in J \implies x+y \in I \land x+y \in J \implies x+y \in I \cap J$
  - $x \in I \land x \in J \implies -x \in I \land -x \in J \implies -x \in I \cap J$
- $a \in A, x \in I \cap J \implies ax \in I \cap J$, poiché:

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

Definition 13. Prodotto tra ideali

Dati due ideali $I, J \subseteq A$, definiamo il loro prodotto come:

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

Dimostrazione:

- $I \cap J$ è sottogruppo di A, poiché:
  - $0 \in I \land 0 \in J \implies 0 = 0 + 0 \in I \cdot J$
  - $x = i_1 j_1 + i_2 j_2 + \ldots + i_n j_n \in I \cdot J, , y = i'_1 j'_1 + i'_2 j'_2 + \ldots + i'_n j'_n \in I \cdot J \implies x + y = i_1 j_1 + i'_1 j'_1 + \ldots + i_n j_n + i'_n j'_n \in I \cdot J$
  - $x \in I \cdot J \implies -x = x = (-i_1) j_1 + (-i_2) j_2 + \ldots + (-i_n) j_n \mid -i_k \in I, j_h \in J \implies -x \in I \cdot J$
- $a \in A, x \in I \cdot J \implies ax \in I \cdot J$, poiché:

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

Capitolo 2

Numeri Complessi

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

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

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

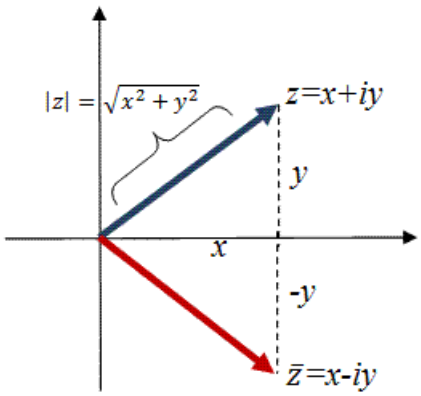
Ovviamente, da tale definizione di insieme dei numeri complessi ne segue che $\mathbb{R} \subseteq \mathbb{C}$, poiché $\forall a \in \mathbb{R} \implies \exists z \in \mathbb{C} \mid z = a + i \cdot 0 = a$. Inoltre, definiamo un **numero immaginario puro** come un numero nella forma $z \in \mathbb{C}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

Definition 14

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

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

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



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

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

Observation 3

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

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

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

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

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

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

2.1 Il campo dei numeri complessi

Proposition 1

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

Dimostrazione:

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

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

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

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

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

- È un gruppo abeliano nella somma:
  - **Associatività della somma**

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

$$= a + bi + c + di + e + fi = a + bi + (c + di + e + fi) = z + (w + q)$$

  - **Elemento neutro della somma**

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

  - **Elemento inverso della somma**

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

  - **Commutatività della somma**

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

- È un gruppo abeliano nel prodotto:
  - **Associatività del prodotto**

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

  - **Elemento neutro del prodotto**

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

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

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

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

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

  - **Commutatività del prodotto**

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

2.2 Forma polare dei numeri complessi

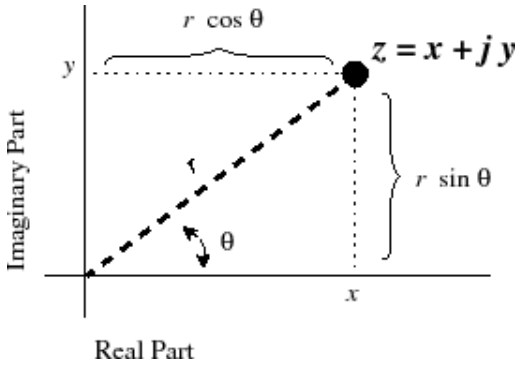
Inoltre, abbiamo visto come un numero complesso possa essere espresso come un punto sul piano gaussiano tramite una **coppia di valori**, descrivendo la distanza di tale punto dall'origine del piano $(0, 0)$ come $|z|$.

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

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

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

Graficamente, ciò corrisponde a dire che:



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

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

Considerato il sistema imposto, dato un numero $z = a + ib \in \mathbb{C}$, possiamo riscrivere tale numero complesso nella sua **forma polare**, ossia

Definition 15. Forma polare dei numeri complessi

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

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

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

Utilizziamo anche la **notazione contratta**:

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

dunque:

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

Giustificazione per la notazione contratta:

- Matematicamente, tramite le proprietà degli esponenti abbiamo che

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

- Svolgiamo ora tale calcolo tramite la notazione esplicita

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

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

- Tramite le proprietà trigonometriche, in particolare $\cos(a+b) = \cos(a)\cos(b) - \sin(a)\sin(b)$ e $\sin(a+b) = \cos(a)\cos(b) + \sin(a)\sin(b)$, riscriviamo tale espressione come:
$$\cos(\theta_1 + \theta_2) + i \cdot \sin(\theta_1 + \theta_2)$$
- Riscrivendo il risultato nella forma contratta, otteniamo che i due calcoli matematici risultano essere equivalenti tra di loro:
$$\cos(\theta_1 + \theta_2) + i \cdot \sin(\theta_1 + \theta_2) = e^{i(\theta_1+\theta_2)}$$

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

Definition 16. Formula di De Moivre

Dato $z \in \mathbb{C}$, si ha che:
$$z = re^{i\theta} \implies z^n = (re^{i\theta})^n = r^n e^{in\theta}$$

Esempi:

1. Dato $z = -i$, calcolare z^4.
   - Calcoliamo l'argomento principale di z: $|z| = \sqrt{0^2 + (-1)^2} = 1$
   $$\begin{cases} \cos(\theta) = \frac{0}{1} = 0 \\ \sin(\theta) = \frac{-1}{1} = -1 \end{cases} \implies Arg(z) = \frac{3}{2}\pi \implies arg(z) = Arg(z) + 2k\pi, k \in \mathbb{Z}$$
   - Quindi, riscriviamo z come
   $$z = re^{Arg(z)\cdot i} = e^{\frac{3}{2}\pi \cdot i}$$
   - A questo punto, z^4 corrisponderà a:
   $$z^4 = e^{4\cdot\frac{3}{2}\pi\cdot i} = e^{6\pi\cdot i} = e^{0\cdot i} = 1$$
2. Dato $z = 1 - i$, calcolare z^{10}.
   - Calcoliamo l'argomento principale di z: $|z| = \sqrt{1^2 + (-1)^2} = \sqrt{2}$
   $$\begin{cases} \cos(\theta) = \frac{1}{\sqrt{2}} \\ \sin(\theta) = \frac{-1}{\sqrt{2}} \end{cases} \implies Arg(z) = \frac{7}{4}\pi \implies arg(z) = Arg(z) + 2k\pi, k \in \mathbb{Z}$$
   - Quindi, riscriviamo z come
   $$z = re^{Arg(z)\cdot i} = \sqrt{2}e^{\frac{7}{4}\pi\cdot i}$$

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

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

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

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

2.3 Teorema fondamentale dell'algebra

Considerati due numeri z e n dove $z \in \mathbb{C}$ e $n \in \mathbb{N}, n \geq 2$, ci chiediamo quante siano le **soluzioni complesse dell'equazione** $x^n = z$.

Nel caso in cui $z = 0$, l'unica soluzione risulta essere $x = 0$. Nel caso in cui $z \neq 0$, invece, esistono n **distinte soluzioni**.

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

$$x^n = z$$

$$x = \sqrt[n]{z}$$

$$x = z^{\frac{1}{n}}$$

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

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

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

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

Esempio:

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

$$x^3 = i \implies x^3 = e^{\frac{1}{2}\pi i}$$

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

- Se $k = 0$

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

- Se $k = 1$

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

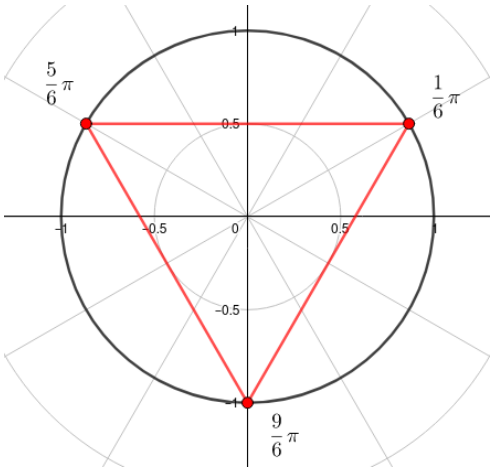
- Se $k = 2$

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

- Se $k = 3$
$$x_4 = e^{i(\frac{1}{2\cdot 3}\pi + \frac{6\pi}{3})} = e^{i(\frac{1}{6}\pi + 2\pi)} = e^{\frac{1}{6}\pi i} \implies x_4 = x_1$$
- Se $k = 4$
$$x_5 = e^{i(\frac{1}{2\cdot 3}\pi + \frac{8\pi}{3})} = e^{i(\frac{1}{6}\pi + \frac{2\pi}{3} + 2\pi)} = e^{\frac{5}{6}\pi i} \implies x_5 = x_2$$
- ...

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

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



Observation 4

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

Infine, concludiamo il nostro studio sui numeri complessi affermando il seguente **teorema fondamentale dell'algebra**

Theorem 2. Teorema fondamentale dell'algebra

Dato un polinomio del tipo:

$$p(x) := a_0 + a_1 x + \ldots + a_n x^n = 0$$

dove $a_i \in \mathbb{C}, n \geq 1, a_n \neq 0$, **esistono sempre** n **radici complesse** di $p(x)$:

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

Capitolo 3

Relazioni e Induzione

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

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

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 $\not R\,(x, y)$).

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

Tra le varie proprietà che possono essere soddisfatte da una relazione, in particolare evidenziamo:

- **Riflessività**: $x \sim x, \forall x \in S$
- **Simmetria**: $x \sim y \implies y \sim x, \forall x, y \in S$
- **Anti-simmetria**: $x \sim y \land y \sim x \implies x = y, \forall x, y \in S$
- **Transitività**: $x \sim y \land y \sim z \implies x \sim z, \forall x, y, z \in S$

Definition 17. Relazione di equivalenza

Una relazione viene detta **relazione di equivalenza** se su di essa valgono le proprietà di **riflessività**, **simmetria** e **transitività**.

Esempi:

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

Definition 18. Relazione d'ordine

Una relazione viene detta **relazione d'ordine parziale** se su di essa valgono le proprietà di **riflessività**, **anti-simmetria** e **transitività**.

Nel caso in cui $\forall x, y \in S$ vale $x \sim y \vee y \sim x$, definiamo tale relazione come **relazione d'ordine totale**.

Esempi:

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

  $$P(X) = \{\texttt{tutti i sottoinsiemi di } X\}$$

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

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

    $$A \subseteq A \quad \forall A \in P(X)$$

  - 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 $\{1\} \not\subseteq \{2\}$

3.1 Classi di equivalenza

Definition 19

Data una relazione d'equivalenza $\sim$ definita su un insieme S, denotiamo con $[x]$ la sua **classe di equivalenza**, dove $[x] \subseteq S$ e $x \in S$, l'insieme di tutti gli elementi in relazione con x:

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

Observation 5

Ogni classe di equivalenza possiede **almeno un elemento**, poiché per riflessività vale che $x \sim x \implies x \in [x]$

Observation 6

Tutte le classi di equivalenza indotte da una relazione su un insieme X **sono disgiunte tra loro**

Dimostrazione:

- Supponendo $x \sim y$, se $z \in [x] \implies z \sim x$ allora $z \sim y \implies z \in [y]$, dunque $[x] \subseteq [y]$. Effettuando il ragionamento opposto, ne traiamo che $[y] \subseteq [x]$ e dunque che
$$x \sim y \iff [x] = [y]$$
- Supponiamo per assurdo che $z \in [x] \cap [y]$. Ciò significa che $z \in [x] \land z \in [y] \iff z \sim x \land z \sim y$. Poiché per simmetria si ha che $z \sim x \iff x \sim z$, per transitività concludiamo che $x \sim z, z \sim y \implies x \sim y$ Dunque, concludiamo che:
$$x \nsim y \iff [x] \cap [y] = \emptyset$$

Definition 20. Insieme quoziente

Data una relazione di equivalenza $x \sim y$, definiamo l'insieme di tutte le classi di equivalenza indotte sull'insieme X come

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

Definition 21. Partizionamento di un insieme

Dato un insieme X e un insieme di n indici $I : \{0, \dots, n\}$, una **partizione di** X è un sottoinsieme di X disgiunto da tutte le altre partizioni di X:

$$X = \bigcup_{i \in I} X_i \text{ dove } i \neq j \implies X_i \cap X_j = \emptyset$$

Denotiamo il partizionamento di un insieme X con il simbolo di **unione disgiunta** (ossia unione di insiemi disgiunti):

$$X = \coprod_{i \in I} X_i$$

Proposition 3

Applicare una **relazione di equivalenza** su un insieme equivale a **partizionare** tale insieme, poiché ogni classe di equivalenza è un sottoinsieme di X disgiunto da tutte le altre classi.

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

Inoltre, dato un partizionamento di X, otteniamo una relazione di equivalenza $\sim$ su di esso:

- **Riflessività**:
$$\forall x \in X, \exists i \in I \mid x \in X_i \implies x \sim x$$
- **Simmetria**:
$$x \sim y, \exists i, j \in I \mid x, y \in X_i \implies x, y \in X_j \implies y \sim x$$
- **Transitività**:
$$x \sim y, y \sim z, \exists i, j \in I \mid x, y \in X_i, y, z \in X_j \implies y \in X_i \cap X_j$$

  Tuttavia, poiché le partizioni sono disgiunte tra loro, abbiamo che $i \neq j \implies X_i \cap X_j = \emptyset$, quindi si può verificare solo che $i = j \implies X_i = X_j$, dunque otteniamo che $x \sim z$.

Proposition 4. Proiezione al quoziente

Applicare una relazione di equivalenza su un insieme X equivale all'applicazione di una funzione suriettiva detta **proiezione al quoziente**:

$$\rho : X \to X/\sim : x \mapsto [x]$$

3.2 Relazione di Divisore

Definition 22. Relazione di divisore

Dati due numeri naturali $m, n \in \mathbb{Z}$, affermiamo che "m è divisore di n", indicato come $m \mid n$ (*Attenzione: non è il simbolo matematico "tale che"*), se esiste un elemento $p \in \mathbb{Z} \mid m \cdot p = n$:

$$m \mid n \iff \exists p \in \mathbb{Z} m \cdot p = n$$

Analizziamo le proprietà della relazione definita:

- Soddisfa la **riflessività**:
$$m \mid m \quad \forall m \in \mathbb{Z} \implies m \cdot 1 = m$$

- Soddisfa la **transitività**:

$$d \mid m \implies \exists p \in \mathbb{Z}, d \cdot p = m$$

$$m \mid n \implies \exists q \in \mathbb{Z}, m \cdot q = n$$

$$d \mid m, m \mid n \implies n = m \cdot q = d \cdot p \cdot q = d \cdot (pq) \implies d \mid n$$

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

$$m \mid n \implies \exists p \in \mathbb{Z}, m \cdot p = n$$

$$n \mid m \implies \exists q \in \mathbb{Z}, n \cdot q = m$$

$$m \mid n, n \mid m \implies m = n \cdot q = m \cdot p \cdot q$$

  a questo punto, si hanno due casi:

  - $m = 0 \implies n = p = q = 0$
  - $m \neq 0 \implies p \cdot q = 1 \implies p = q = \pm 1$
    - Se $p = q = 1 \implies m = n$
    - Se $p = q = -1 \implies m = -n$

  Dunque, deduciamo che non in tutti i casi la relazione $\mid$ risulta essere anti-simmetrica.

- Nel caso in cui la relazione venisse applicata su $\mathbb{N}$ invece che $\mathbb{Z}$, il caso in cui $p = q = -1$ verrebbe scartato, poiché $-1 \notin \mathbb{N}$, rendendo quindi la relazione anti-simmetrica e, di conseguenza, anche una relazione d'ordine parziale.

3.3 Relazione di Congruenza

Definition 23. Relazione di congruenza

Dato $n \in \mathbb{N}, n \geq 2$ e dati $a, b \in \mathbb{Z}$ denotiamo con $a \equiv b (\texttt{mod}\ n)$ la relazione "a è congruente b modulo n" se e solo se $n \mid b - a$

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

Esempi:

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

La relazione risulta essere una relazione di equivalenza:

- **Riflessiva**:

$$0 = n \cdot 0 \implies n \mid 0 \implies n \mid a - a \implies a \equiv a (\texttt{mod}\ n) \quad \forall a \in \mathbb{Z}$$

- **Simmetrica**:

$$a \equiv b(\mathsf{mod}\ n) \implies n \mid b-a \implies \exists p \in \mathbb{Z}, b-a = n \cdot p \implies$$
$$\implies a-b = n \cdot (-p) \implies n \mid a-b \implies b \equiv a(\mathsf{mod}\ n)$$

- **Transitiva**:

  Siccome:

$$a \equiv b(\mathsf{mod}\ n), b \equiv c(\mathsf{mod}\ \mathsf{n}) \implies b-a = n \cdot p, c-b = n \cdot q$$

  allora:

$$c-a = (c-b)+(b-a) = q \cdot n + p \cdot n = n(q+p) \implies n \mid c-a \implies a \equiv c(\mathsf{mod}\ n)$$

3.4 Teorema della divisione con resto euclidea

Theorem 5. Teorema della divisione con resto euclidea

Dati due interi $m, n \in \mathbb{Z}$ dove $n > 0$, allora

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

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

Dimostrazione dell'unicità:

- Supponiamo che q ed r non siano unici. Allora, ne segue che:

$$nq_1 + r_1 = m = nq_2 + r_2 \implies r_2 - r_1 = n(q_1 - q_2) \implies n \mid r_2 - r_1$$

- Siccome $0 \leq r_1, r_2 < n \implies -n < r_2 - r_1 < n$ e siccome $n \mid r_2 - r_1$, ciò significa che $r_2 - r_1$ deve essere un multiplo di n compreso tra $-n$ ed n stesso. Poiché l'unico numero rispettante tali caratteristiche è 0, ne segue che:

$$r_2 - r_1 = 0 \implies r_2 = r_1$$

- Quindi, otteniamo che:

$$nq_1 + r_1 = nq_2 + r_2 \implies nq_1 = nq_2 \implies q_1 = q_2$$

Dimostrazione dell'esistenza:

- Sia $[m]$ la **classe di congruenza** di $m(\mathsf{mod}\ n)$:

$$[m] : \{a \in \mathbb{Z} \mid a \equiv m(\mathsf{mod}\ n)\}$$

- Allora, abbiamo che:

$$n \mid m-a \implies m-a = n \cdot p \implies a = m - np$$

- Sia r il minimo valore tra le $a \in [m]$, dove $a > 0$. Quindi, vale che

$$\exists r \in \mathbb{Z} \mid r = m - nq \implies m = nq - r$$

- Verifichiamo ora che $0 \leq r < n$. Assumiamo per assurdo che $r \geq n$, allora ne segue che $r - n \geq 0$. Quindi abbiamo che:

$$r-n = (m-nq)-n = m-(q+1)n \implies m-(q+1)n \in [m] \implies r \text{ non è il minimo valore}$$

3.5 Relazione di Coniugio

Definition 24. Relazione di coniugio

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

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

Observation 7

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

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

Observation 8

La relazione di coniugio è una relazione di equivalenza.

Dimostrazione:

- **Riflessività**:

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

- **Simmetria**:

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

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

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

- **Transitività**:

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

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

Per esprimere tale concetto matematicamente, possiamo dire che:

Definition 25. Principio di induzione

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

$$p_1) \implies p_2)$$

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

$$...$$

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

Esempi:

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

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

   - 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 $p_{n+1})$:

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

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

$$\underbrace{1+2+3+...+n}_{\text{Ipotesi induttiva}}+(n+1)=\frac{(n+1)(n+1+1)}{2}$$

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

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

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

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:

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

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

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

- Verifichiamo quindi p_0) e p_1:

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

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

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

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

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

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

verificando quindi la validità del passo induttivo

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

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

dove il coefficiente binomiale è definito come:

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

- Verifichiamo quindi il caso base:

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

- A questo punto effettuiamo il passo induttivo:

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

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

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

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

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

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

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

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

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

- A questo punto uniamo nuovamente le due sommatorie:

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

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

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

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

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

Capitolo 4

Elementi di Teoria degli Anelli

4.1 Insieme quoziente

4.1.1 Classi laterali sinistre

Sia $(G, \cdot)$ un gruppo e sia $H \subseteq G$ sottogruppo. Definiamo la seguente relazione $x \sim y \iff x^{-1}y \in H$, verificando che essa sia una relazione di equivalenza:

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

Definiamo quindi un particolare tipo di classi di equivalenza:

Definition 26. Classi laterali sinistre

Data la relazione di equivalenza $x \sim y \iff x^{-1}y \in H$, definiamo come **classi laterali sinistre** di G in H le classi di equivalenza generate da tale relazione:

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

Denotiamo come G/H (pronunciato G modulo H) l'insieme quoziente di tutte le classi laterali sinistre generate da H su G.

Esempio:

- Sia $I(3) \subseteq \mathbb{Z}$ il sottogruppo contenente tutti i multipli di 3. In tal caso, l'insieme quoziente $\mathbb{Z}/I(3)$ verrà partizionato in tre classi laterali sinistre:

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

  In particolare, notiamo come:

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

- Più in generale, si verifica che:

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

Definition 27. Insieme quoziente $\mathbb{Z}_n$

Dato il gruppo abeliano $(\mathbb{Z}, +)$ e il sottoinsieme $I(n) : \{nk \mid k \in \mathbb{Z}\}$, l'insieme quoziente $\mathbb{Z}/I(n)$ **coincide** con l'insieme di classi di equivalenza indotto dalla relazione di congruenza $(\mathbb{Z}/\equiv)$.

Tale particolare insieme quoziente viene indicato come **insieme $\mathbf{Z_n}$**

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

Dimostrazione:

- Abbiamo già dimostrato che $I(n) \subseteq \mathbb{Z}$ è sottogruppo
- Applicando la relazione delle classi laterali sinistre su $I(n)$, in tal caso otteniamo che:

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

$$\implies n \mid b - a \implies a \equiv b (\mathsf{mod}\ n)$$

- Procedendo all'inverso, otteniamo che:

$$a \equiv b(\texttt{mod } n) \implies n \mid b-a \implies b-a = nk, \exists k \in \mathbb{Z} \implies$$

$$\implies b-a = (-a)+b \in I(n) \implies a \sim b$$

Observation 9

Ogni classe laterale sinistra appartenente a G/H corrisponde all'insieme:

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

Dimostrazione:

- Dimostriamo che $[x] \subseteq xH$:

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

  Allora abbiamo che:

$$h = x^{-1}y$$
$$xh = x(x^{-1}y)$$
$$xh = y$$

  Dunque, abbiamo che $y \in xH \implies [x] \subseteq xH$

- Dimostriamo che $xH \subseteq [x]$:

$$y \in xH \implies \exists h \in H, y = xh$$

  Allora abbiamo che:

$$y = xh$$
$$x^{-1}y = x^{-1}(xh)$$
$$x^{-1}y = h$$

  Dunque, abbiamo che $x^{-1}y = h \in H \implies x \sim y \implies y \in [x] \implies xH \subseteq [x]$

Observation 10

Tutte le classi laterali sinistre di H su G hanno la **stessa cardinalità**, corrispondente a $|H|$.

Dimostrazione:

- Poiché $[x] = xH, \forall [x] \in G/H$, allora si ha che:

$$xh, xk \in xH \iff xh \neq xk \iff h \neq k$$

- Di conseguenza, la funzione di proiezione al quoziente $\rho : H \to xH : h \mapsto xh$ è sia suriettiva (per definizione stessa di xH), sia iniettiva (poiché $h \neq k \implies \varphi(h) \neq \varphi(k)$).
- Poiché φ è biettiva, ogni elemento di H viene mandato in un elemento di xH, implicando quindi che:

$$|H| = |xH| = |[x]|, \forall [x] \in G/H$$

4.1.2 Teorema di Lagrange

Theorem 6. Teorema di Lagrange

Sia G un **gruppo finito** e sia $H \subseteq G$ sottogruppo (dunque anche H finito). In tal caso, si ha che:

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

Dimostrazione:

- Poiché le classi laterali sinistre di G in H sono classi di equivalenza, possiamo partizionare G in $|G/H|$ partizioni:

$$G = \coprod_{[x] \in G/H} [x]$$

- Siccome $|[x]| = |H|, \forall [x] \in G/H$, allora la cardinalità di G corrisponde a:

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

4.2 L'anello commutativo $\mathbb{Z}_n$

Proposition 7. Gruppo quoziente G/H

Sia $(G, +)$ un **gruppo abeliano** e sia $H \subseteq G$ **sottogruppo**. In tal caso, anche l'insieme quoziente $(G/H, +)$ è un **gruppo abeliano**.

Dimostrazione:

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

$$[x] = [x'], [y] = [y'] \implies x \sim x', y \sim y' \implies x' - x, y' - y \in H \implies$$
$$\implies (x'-x)+(y'-y) = (x'+y')-(x+y) \in H \implies x+y \sim x'+y' \implies [x+y] = [x'+y']$$

- Verifichiamo quindi gli assiomi di gruppo abeliano:
  - **Associatività**:
    $$([x]+[y])+[z]=[x+y]+[z]=[x+y+z]=[x]+[y+z]=[x]+([y]+[z])$$
  - **Elemento neutro**:
    $$[x]+[0]=[x+0]=[x]$$
  - **Elemento inverso**:
    $$[x]+[-x]=[x+(-x)]=[0]$$
  - **Commutatività**:
    $$[x]+[y]=[x+y]=[y+x]=[y]+[x]$$

Corollary 1

L'insieme quoziente $\mathbb{Z}_n$ è un gruppo abeliano nella somma

Esempi:

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

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

Proposition 8. Anello quoziente A/I

Sia $(A,+,\cdot)$ un **anello commutativo** e sia $I \subseteq A$ **ideale**. In tal caso, anche $(A/I,+,\cdot)$ è un **anello commutativo**.

Dimostrazione:

- Abbiamo già visto che $(A/I,+)$ è gruppo abeliano e che $+ : A/I \times A/I \to A/I$ è ben definita
- Verifichiamo quindi che $\cdot : A/I \times A/I \to A/I$ sia ben definita, dunque che valga:
  - $x \equiv x'(\mathtt{mod}\ I) \implies i_1 := x'-x \in I$
  - $y \equiv y'(\mathtt{mod}\ I) \implies i_2 := y'-y \in I$
  - $xy \equiv x'y'(\mathtt{mod}\ I) \implies x'y'-xy \in I$

  $$x'y'-xy=x'y'+xy'-xy'-xy=(x'-x)y'+x(y'-y)=i_1y'+xi_2$$

  Siccome $i_1y', xi_2 \in I$ ne segue che $x'y'-xy=i_1y'+xi_2 \in I$, l'operazione prodotto è ben definita.

- Ammette l'assioma di associatività nel prodotto:

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

- Ammette l'assioma di elemento neutro nel prodotto:

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

- Ammette l'assioma di commutatività nel prodotto:

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

Corollary 2

L'insieme quoziente $\mathbb{Z}_n$ è un anello commutativo nella somma con il prodotto

Esempi:

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

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

4.3 Invertibili e Divisori dello zero

Definition 28. Elementi invertibili

Dato un anello commutativo $(A, +, \cdot)$ e dato un elemento $a \in A$, affermiamo che a è **invertibile** se e solo se $\exists a^{-1} \in A \mid aa^{-1} = a^{-1}a = 1$.

Denotiamo come A^* l'**insieme degli invertibili** di A.

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

Definition 29. Divisori dello zero

Dato un anello commutativo $(A, +, \cdot)$ e dato un elemento $a \in A$, affermiamo che a un **divisore dello zero** se e solo se $a \mid 0 \iff 0 = ab, \exists b \in A$.

Affermiamo che A è un **dominio di integrità** se l'unico elemento divisore dello zero è lo zero stesso ($\nexists a \neq 0 \in A$ tale che $a \mid 0$)

Observation 11

Un elemento è **invertibile** se e solo se **non è un divisore dello zero** (dunque può essere un divisore dello zero se e solo se non è un invertibile)

Dimostrazione per assurdo:

- Supponiamo che $\exists a, b \in A^*, b \neq 0 \mid ab = 0$. Allora, abbiamo che:

$$b = 1 \cdot b = (aa^{-1})b = a^{-1}(ab) = a^{-1} \cdot 0 = 0 \implies b = 0$$

  contraddicendo quindi l'ipotesi iniziale, ossia $b \neq 0$

Observation 12

A può essere un dominio di integrità se e solo se vale la **legge di annullamento del prodotto**, ossia $xy = 0 \iff x = 0 \vee y = 0$

Observation 13

$(A^*, \cdot)$ è un gruppo, poiché:

- L'elemento neutro 1 è invertibile, infatti $1^{-1} = 1 \implies 1 \in A^*$
- $x, y \in A^* \implies (xy)^{-1} = y^{-1}x^{-1} \implies xy \in A^*$
- $x \in A^* \implies x = (x^{-1})^{-1} \in A^* \implies x^{-1} \in A^*$

Observation 14

Se A è un **campo**, allora esso è **sempre un dominio di integrità**, poiché in tal caso si ha $A - A^* = \{0\}$, poiché ogni elemento di un campo è invertibile, dunque 0 è l'unico divisore dello zero esistente.

Proposition 9

Sia A un dominio di integrità. Dati $a, b \in A$, si verifica che:

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

Dimostrazione:

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

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

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

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

  Dunque si verifica che:

$$a = bc = adc \implies a = adc \implies a(1 - dc) = 0 \implies$$

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

Corollary 3

Nell'anello commutativo $\mathbb{Z}$, si verifica che:

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

Dimostrazione:

- $a = \pm b \implies I(a) = I(b)$:

$$x \in I(a) \implies \exists y \in \mathbb{Z} \mid x = ay \implies -x = -(ay) = (-a)y \in I(-a)$$

- $I(a) = I(b) \implies a = \pm b$:

$$I(a) = I(b) \implies a \in I(b), b \in I(a) \implies p, q \in \mathbb{Z} \mid a = bp, b = qa \implies$$

$$\implies a = (qa)a \implies pq = 1 \implies p = q = \pm 1$$

Quindi gli unici due casi possibili sono:

$$p = q = 1 \implies a = b$$

$$p = q = -1 \implies a = -b$$

4.3.1 Irriducibili e Primi

Definition 30. Irriducibili e Primi

Dato un anello commutativo A e un elemento $a \in A$.

- L'elemento a viene detto **irriducibile** se:
  - $a \neq 0 \wedge a \notin A^*$
  - $a = bc \implies b \in A^* \vee c \in A^*$
- L'elemento a viene detto **primo** se:
  - $a \neq 0 \wedge a \notin A^*$
  - $a \mid bc \implies a \mid b \vee a \mid c$

Proposition 10

Se A è un dominio di integrità e $a \in A$ è **primo**, allora esso è **anche irriducibile** (non è detto il contrario)

$$a \in A \mid a \texttt{ primo} \implies a \texttt{ irriducibile}$$

Dimostrazione:

- Supponiamo che $a \in A$ sia primo. La prima condizione è condivisa da entrambe le definizioni, quindi è automaticamente verificata.
- Supponiamo che $a = bc$. In tal caso, si ha che $a \mid a \implies a \mid bc \implies a \mid b \vee a \mid c$
- A questo punto, si ha che:

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

- Siccome $a \neq 0$, allora:

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

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

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

Observation 15

$\mathbb{Z}_n$ è un dominio di integrità se e solo se n è un numero primo.

In tal caso, usiamo la notazione $\mathbb{Z}_p$ per dire che si tratta dell'anello quoziente di un numero primo.

Dimostrazione:

- $\mathbb{Z}_n$ dominio $\implies$ n primo
  - Supponiamo che n non sia primo, ossia che possa essere espresso come il prodotto di due fattori ab tali che $a \notin A^* \wedge b \notin A^*$:

$$n = ab, 0 < a, b < n \implies [n] = [ab] = [a][b]$$

  - Tuttavia, in $\mathbb{Z}_n$ abbiamo che $[n] = [0]$, implicando che $[n] = [ab] = [0]$.
  - Per la legge di annullamento del prodotto, $[a][b] = [0] \implies [a] = [0] \vee [b] = [0]$, contraddicendo l'ipotesi $a, b > 0$
- Di conseguenza, si ha che $a \mid 0$ e $b \mid 0$, dunque $\mathbb{Z}_n$ non può essere un dominio di integrità.

4.4 Massimo comun divisore

Definition 31. Massimo comun divisore (MCD)

Sia I un ideale di $\mathbb{Z}$, allora esiste un $\exists! d \geq 0$ tale che $I = I(d)$ dove $I(d) : \{ad \mid a \in \mathbb{Z}\}$. Il generatore d di tale ideale principale viene definito come **massimo comun divisore**

$$d := MCD(a_1, \ldots, a_n)$$

In altre parole, si ha che:

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

che definiamo come **identità di Bezout**.

Dimostrazione:

- Se $I : \{0\}$, allora $I = I(0)$. Nel caso contrario, si avrebbe che $I \cap \mathbb{Z}_{>0} \neq 0$, infatti $\exists 0 \neq n \in I$ tale che:
  - $n > 0 \implies n \in I$
  - $n < 0 \implies -n > 0 \implies -n \in I$
- Poniamo allora $d := min(I \cap \mathbb{Z}_{>0})$ e mostriamo che $I = I(d)$:
  - $I(d) \subseteq I$:
    - $x \in I(d) \implies \exists y \in \mathbb{Z} \mid x = yd$
    - Per l'assioma degli ideali $IA \subseteq I$, ne segue che $d \in I$
  - $I \subseteq I(d)$:
    - $x \in I$
    - La divisione con resto di x per d, dove $d \neq 0$, equivale a :
      $$\exists! q \in Z, 0 \leq r < d \mid x = dq + r$$
    - Assumiamo per assurdo che $r \neq 0$. Allora abbiamo che:
      $$r \in I \cap \mathbb{Z}_{>0} \wedge r < d$$
      dunque contraddicendo la definizione $d := min(I \cap \mathbb{Z}_{>0})$
    - Dunque l'unica possibilità che $r = 0$:
      $$x = dq + r \implies r = x - dq \implies x \in I, dq \in I(d)$$
    - A questo punto, seguiamo la dimostrazione del punto precedente per verificare che $dq \in I(d) \implies dq \in I$
- Affermiamo quindi che dati $a_1, ..., a_n \in \mathbb{Z}$, il loro $d := MCD(a_1, ..., a_n)$ è l'**unico intero** $d \geq 0 \mid I(d) = I(a_1, ..., a_n)$.

Observation 16

Tale definizione di MCD coincide con la "classica" matematica, poiché:

$$d \mid x, \forall x \in I(d) = I(a_1, ..., a_n)$$

Dimostrazione:

Verifichiamo che $e \mid a_1, ..., e \mid a_n \implies e \mid d$, dove ricordiamo che e è l'elemento neutro e $e \mid a_i \implies \exists x \in \mathbb{Z}, a_i = ex_1$:

$$d \in I(a_1, ..., a_n) \implies \exists b_1, ..., b_n \mid \underbrace{d = a_1b_1 + ... + a_nb_n}_{\text{Identità di Bezout}} =$$
$$= (ex_1)b_1 + ... + (ex_n)b_n = e(xb_1 + ... + xb_n) \implies e \mid d$$

Definition 32. Dominio ad ideali principali

Un dominio di integrità in cui **ogni ideale I è principale**, ossia esiste sempre un ideale principale $I(x) \mid I = I(x)$, viene detto **dominio ad ideali principali**.

Corollary 4

$\mathbb{Z}$ è un **dominio ad ideali principali**, poiché $I = I(d)$ dove $d := MCD(a_1, \ldots, a_n)$

Proposition 11

Dato l'anello $(\mathbb{Z}_n, +, \cdot)$ e dato $0 < a < n$ abbiamo che:

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

Dimostrazione:

- Verifichiamo che $[a] \in \mathbb{Z}_n^* \implies MCD(a, n) = 1$. Supponendo che $[a] \in \mathbb{Z}_n^*$ abbiamo che:

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

  Sia $d := MCD(a, n) > 0$. Dunque abbiamo 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 $d > 0$, il caso con $d = p = -1$ viene escluso, dunque l'unico caso possibile è $d = p = 1$

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

  Supponendo che $MCD(a, n) = 1$ abbiamo che:

  $$I(d) = I(a, n) \implies d \in I(a, n) \implies \exists b, k, d = ab + nk$$

Considerando le classi di congruenza modulo n, dove quindi $[n] = [0]$, otteniamo:

$$[1] = [ab + nk] = [a][b] + [n][k] = [a][b] \implies [b] = [a]^{-1} \implies [a] \in \mathbb{Z}_n^*$$

Corollary 5

Dato p un numero primo, $\mathbb{Z}_p$ **è un campo** poiché

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

Corollary 6

Dato un **campo** K e dato $a \in K, a \neq 0$, l'**equazione** $ax = b$ **ammette sempre la soluzione** $x = ba^{-1}$, poiché esiste sempre un inverso di a.

Esempio:

- Nel campo $\mathbb{Z}_7$ risolviamo l'equazione $[3]x + [2] = [0]$:

$$[3]x + [2] = [0] \implies [3]x = -[2] \implies [3]x = [5] \implies$$
$$\implies x = [5][3]^{-1} \implies x = [5][5] \implies x = [25] \implies x = [4]$$

  Poiché in $\mathbb{Z}_7$ l'inverso nel prodotto $[3]^{-1}$ corrisponde a $[5]$ ($[3][5] = [15] = [1]$)

Theorem 12

Data la seguente equazione:

$$ax \equiv b (\mathsf{mod}\ n)$$

Sia $d := MCD(a, n)$. Si verifica che:

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

$$px \equiv q (\mathsf{mod}\ m)$$

Dimostrazione:

- Se l'equazione ammette una soluzione $x \in \mathbb{Z}$, allora $ax = b + nk, \exists k \in \mathbb{Z}$.
- Poiché $d \mid a$ e $d \mid n$ (dato che $d := MCD(a, n)$), allora si ha che $d \mid b = ax - nk$. 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:

$$ax \equiv b (\mathsf{mod}\ n) \iff pdx \equiv qd (\mathsf{mod}\ md) \iff$$
$$\iff dpx = dq + dmk, \exists k \in \mathbb{Z} \iff px = q + mk \iff px \cong q (\mathsf{mod}\ m)$$

4.4.1 Algoritmo di Euclide

Siano $a, b \in \mathbb{Z}$ e sia $d := MCD(a, b)$. Poiché $I(a, b) = I(-a, b) = I(a, -b) = I(-a, -b)$, possiamo supporre che $0 < a, b$. Inoltre, poiché $I(a, b) = I(b, a)$, $MCD(0, b) = b$ e $MCD(a, 0) = 0$, supponiamo che $0 < a \leq b$.

Definiamo quindi **due metodi** per poter calcolare il massimo comun divisore tra due numeri, uno standard ed uno algoritmico:

Method 1. Fattorizzazione standard

- Scomponiamo a e b in **fattori primi**
- La composizione in fattori primi di d equivale ai **fattori in comune col grado minimo tra le due scomposizioni** di a e b

Esempio:

$$MCD(448, 216) = MCD(2^6 \cdot 7, 2^3 \cdot 3^3) = 2^3 = 8$$

Method 2. Algoritmo di Euclide

1. Assumiamo $0 < a \leq b$
2. Poniamo $r_0 := b$ e $r_1 := a$
3. Definiamo **ad ogni iterazione** $r_{i+1} := r_{i-1}(\texttt{mod}\ r_i)$, da cui ne segue che:
$$r_{i-1} = r_i q_i + r_{i+1}$$
4. Viene ripetuto il punto 3 finché $r_{i+1} \neq 0$
5. All'n-esima iterazione, ossia quando $r_{i+1} = 0$, si ha che $MCD(a, b) = r_n$

Dimostrazione:

Vogliamo verificare che $r_n = d := MCD(a, b)$, ossia che $r_n \mid d$ e $d \mid r_n$.

- Verifichiamo che $d \mid r_n$:

  $$d := MCD(a, b) \iff d \mid r_1 \wedge d \mid r_0 \text{ dove } r_1 := a \in I(a, b), r_0 := b \in I(a, b)$$

  Siccome $r_i \in I(a, b), \forall 0 \leq i \leq n$, otteniamo che:

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

  Di conseguenza, abbiamo che $d \mid r_n$

- Verifichiamo che $r_n \mid d$:

  $$r_n \mid r_i, \forall 0 \leq i \leq n \implies i = n, r_n | r_n \wedge r_{n-1} = r_n q_n + 0 \implies r_n | r_{n-1}$$

  Siccome $r_n \mid x, r_n \mid y \implies r_n \mid (cx + dy), \forall c, d \in \mathbb{Z}$, allora:

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

$$r_n \mid r_{n-1} \wedge r_n \mid r_{n-2} \implies r_n \mid r_{n-3}$$
$$\dots$$
$$r_n \mid r_1 \wedge r_n \mid r_0 \implies r_n \mid d$$

dove $d := MCD(a, b)$

Esempi:

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

$$r_0 = r_1 \cdot q_1 + r_2$$
$$448 = 216 \cdot 2 + 16$$
$$216 = 16 \cdot 13 + 8$$
$$16 = 8 \cdot 2 + 0$$

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

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

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

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

$$216x + 448y = 8$$

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

$$216x + 448y = 8$$
$$216x + 448y = 216 - 16 \cdot 13$$
$$216x + 448y = 216 - (448 - 216 \cdot 2) \cdot 13$$
$$216x + 448y = 216(1 + 13 \cdot 2) - 448 \cdot 13$$
$$216x + 448y = 216(27) + 448(-13)$$

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

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

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

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

$$12600 := 8316 \cdot 1 + 4284$$
$$8316 := 4284 \cdot 1 + 4032$$
$$4284 := 4032 \cdot 1 + 252$$
$$4032 := 252 \cdot 16 + 0$$

  dunque $d = 252$

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

$$8316x + 12600y = 252$$

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

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

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

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

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

dunque $x = -3, y = 2$

– $p := MCD(a, d) = MCD(1470, 252)$

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

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

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

dunque $p = 42$

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

$$1470z + 252w = 42$$

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

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

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

dunque $x = -1, y = 6$

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

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

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

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

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

4.4.2 Approfondimento sull'Identità di Bezout

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

Proposition 13

Data l'equazione $ax + by = d$, dove $d := MCD(a, b)$, e date x_0 e y_0 due soluzioni particolari dell'equazione, tutte le soluzioni dell'equazione hanno la forma:

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

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

Dimostrazione:

Innanzitutto, verifichiamo che le soluzioni possibili siano effettivamente valide:

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

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

$$ax_0 + by_0 = d$$

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

$$\begin{cases} ax_0 + by_0 = d \\ ax_1 + by_1 = d \end{cases} \implies (ax_1 + by_1) - (ax_0 + by_0) = d - d \implies$$

$$a(x_1 - x_0) + b(y_1 + y_0) = 0 \implies a(x_1 - x_0) = -b(y_1 - y_0) \implies$$

$$\implies a(x_1 - x_0) = b(y_0 + y_1)$$

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

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

4.4.3 Criteri di divisibilità

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

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

Osserviamo che:

- $10 \equiv 1 (\mathsf{mod}\ 3) \implies 10x \equiv x (\mathsf{mod}\ 3)$
- $10 \equiv 1 (\mathsf{mod}\ 9) \implies 10x \equiv x (\mathsf{mod}\ 9)$
- $10 \equiv -1 (\mathsf{mod}\ 11) \implies 10x \equiv -x (\mathsf{mod}\ 11)$

Quindi:

- In $\mathbb{Z}_3$ si ha che
$$a = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \left[\sum_{i=0}^{k} a_i \cdot (1)^i \right] (\mathsf{mod}\ 3)$$
- In $\mathbb{Z}_9$ si ha che
$$a = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \left[\sum_{i=0}^{k} a_i \cdot (1)^i \right] (\mathsf{mod}\ 9)$$
- In $\mathbb{Z}_{11}$ si ha che
$$a = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \left[\sum_{i=0}^{k} a_i \cdot (-1)^i \right] (\mathsf{mod}\ 11)$$

Osserviamo inoltre che se $x \equiv y (\mathsf{mod}\ n)$ e $k \mid n$ allora si ha che

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

Esempi:

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

  $129383716 \equiv [6+1+7+3+8+3+9+2+1] (\mathsf{mod}\ 3) \implies 129383716 \equiv 40 (\mathsf{mod}\ 3)$

  Tuttavia, siccome $3 \nmid 40$, ne segue che $3 \nmid 129383716$
- Vogliamo sapere se $3 \mid 129383716$. Siccome siamo in $\mathbb{Z}_{11}$ abbiamo che:

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

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

4.5 Minimo comune multiplo

Ricordando che $\mathbb{Z}$ è un **dominio ad ideali principali** (sezione 4.4), dati due ideali $I = I(a)$ e $J = I(b)$, abbiamo che

- $I + J = I(a) + I(b) = I(a, b) = I(d)$ dove $d := MCD(a, b)$

  Dimostrazione:

  $$I+J = I(a)+I(b) = \{i+j \mid i \in I(a), j \in I(b)\}\} = \{i+j \mid x, y \in \mathbb{Z}, ax = i, by = j\} =$$
  $$= \{ax + by \mid x, y \in \mathbb{Z}\} = I(a, b) = I(d)$$

- $I \cdot J = I(a) \cdot I(b) = I(ab)$

  Dimostrazione:

  - $I(a) \cdot I(b) \subseteq I(ab)$

    $$x \in I(a) \cdot I(b) \implies x = (ax_1)(by_1) + (ax_2)(by_2) + ... + (ax_n)(by_n) =$$
    $$= ab(x_1y_1 + x_2y_2 + ... + x_ny_n) \implies ab \mid x \implies x \in I(ab)$$

  - $I(ab) \subseteq I(a) \cdot I(b)$

    $$x \in I(ab) \implies x = abk = a(bk) \mid a \in I(a), bk \in I(b) \implies x \in I(a) \cdot I(b)$$

- $I(a) \cap I(b) = I(m)$ dove $m := mcm(a, b)$, ossia il **minimo comune multiplo** tra a e b.

Definition 33. Minimo comune multiplo (mcm)

Dati $I(a_1), I(a_2), ..., I(a_n)$, definiamo come $m := mcm(a_1, ..., a_n)$ l'unico intero $m \geq 0$ per cui si ha:

$$I(m) = I(a_1) \cap I(a_2) \cap ... \cap I(a_n)$$

Dunque, caratterizziamo m come il **più piccolo tra i multipli in comune tra** $a_1, a_2, ..., a_n$, avente le proprietà:

$$\begin{cases} a_1 \mid m \wedge a_2 \mid m \wedge ... \wedge a_n \mid m \\ a_1 \mid N \wedge a_2 \mid N \wedge ... \wedge a_n \mid N \end{cases} \implies m \mid N, \forall N = a_1 \cdot ... \cdot a_n$$

Dimostrazione:

- Abbiamo che:

  $$m \in I(m) = I(a_1) \cap I(a_2) \cap ... \cap I(a_n) \implies a_1 \mid m \wedge ... \wedge a_n \mid m$$

- Inoltre, siccome N è multiplo di $a_1, ..., a_n$:

  $$a_1 \mid N \wedge ... \wedge a_n \mid N \implies N \in I(a_1) \cap I(a_2) \cap ... \cap I(a_n) = I(m) \implies m \mid N$$

4.5.1 Teorema fondamentale dell'aritmetica

Il **calcolo del mcm tra due numeri** a, b può essere **ridotto al calcolo del MCD**, tramite il **teorema fondamentale dell'aritmetica**:

Theorem 14. Teorema fondamentale dell'aritmetica

Dati due numeri a e b, si ha che:

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

Attenzione: vale solo se applicato tra due numeri, dunque non vale che $mcm(a_1,..,a_n) \cdot MCD(a1,...,a_n) = a_1 \cdot ... \cdot a_n$

Dimostrazione:

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

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

- Siano quindi $a, b > 0$. Denotiamo l'insieme di tutti i numeri primi come:

$$\mathbb{P} = \{2, 3, 5, 7, 11, ...\}$$

- Considerando $n \in \mathbb{N} \setminus \{0\}$, tale numero può essere scritto come una **fattorizzazione in primi**, ossia:

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

  dove $p \nmid n \implies n_p = 0$

- Riscriviamo quindi a e b come:

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

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

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

- A questo punto, osserviamo che **se uno è il minimo tra i due, l'altro sarà il massimo**:

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

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

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

Corollary 7. Calcolo del mcm

Dati $m := mcm(a,b)$ e $d := MCD(a,b)$, per il teorema fondamentale dell'aritmetica ne segue che

$$m = \frac{ab}{d}$$

4.6 Teorema cinese dei resti

Prima di procedere col teorema riguardante tale sezione, è necessario considerare i seguenti **due lemmi**:

Lemma 15. Numeri coprimi ed mcm

Dati interi $a_1, ..., a_n \geq 2$, se $MCD(a_i, a_j) = 1, \forall i \neq j$ (ossia sono tutti interi coprimi tra loro), allora $mcm(a_1, ..., a_n) = a_1 \cdot ... \cdot a_n$

Dimostrazione:

- Poiché $a_1, ..., a_n$ sono coprimi tra loro, si ha che

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

- Consideriamo anche la loro fattorizzazione in primi:

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

- Dati i due punti precedenti, si ha che:

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

- Ponendo $m := mcm(a_1, ..., a_n)$, quindi, abbiamo che:

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

Lemma 16. Funzione φ

Consideriamo la **notazione** $x \ \texttt{mod q}$, indicante la classe di congruenza $[x]$ modulo q, dove $q \in \mathbb{N}$.

Dati $a_1, ..., a_n \geq 2$ e posto $m := mcm(a_1, ..., a_n)$, la funzione

$$\varphi : \mathbb{Z}_n \to \mathbb{Z}_{a_1} \times \mathbb{Z}_{a_2} \times ... \times \mathbb{Z}_{a_n} : x \ \texttt{mod} \ m \mapsto (x \ \texttt{mod} \ a_1, ..., x \ \texttt{mod} \ a_n)$$

è **ben definita ed iniettiva**

Dimostrazione:

- Consideriamo il sistema:

$$\begin{cases} x \equiv x' (\texttt{mod}\ \ a_1) \\ x \equiv x' (\texttt{mod}\ \ a_2) \\ \vdots \\ x \equiv x' (\texttt{mod}\ \ a_n) \end{cases} \iff \begin{cases} x' - x \in I(a_1) \\ x' - x \in I(a_2) \\ \vdots \\ x' - x \in I(a_n) \end{cases} \iff x' - x \in I(a_1) \cap ... \cap I(a_n)$$

- Poiché $I(a_1) \cap ... \cap I(a_n) = I(m)$, allora:

$$x' - x \in I(a_1) \cap ... \cap I(a_n) = I(m) \iff x \equiv x' (\texttt{mod}\ \ m)$$

Theorem 17. Teorema cinese dei resti

Dati $a_1, ..., a_n \geq 2$ tali che $MCD(a_i, a_j) = 1, \forall i \neq j$ e dove $0 \leq b_i < a_i, 1 \leq i \leq n$, il **sistema di congruenze**

$$\begin{cases} x \equiv b_1 (\texttt{mod}\ \ a_1) \\ x \equiv b_2 (\texttt{mod}\ \ a_2) \\ \vdots \\ x \equiv b_3 (\texttt{mod}\ \ a_n) \end{cases}$$

ammette un'unica soluzione $x \ \texttt{mod}\ q$ dove $m = a_1 \cdot ... \cdot a_n$.

Dimostrazione:

- Sia φ la stessa funzione del primo lemma e sia $m := mcm(a_1, ..., a_n) = a_1 \cdot ... \cdot a_n$ per il secondo lemma.
- Ricordando che l'insieme quoziente in n è definito come $\mathbb{Z}_n : \{0, ..., n-1\}$, la sua cardinalità è $|\mathbb{Z}_n| = n$, calcolando la cardinalità del codominio della funzione φ otteniamo che:

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

- Osserviamo che se il dominio e il codominio di una funzione $f : X \to Y$ hanno la stessa cardinalità finita, ossia $|X| = |Y| < +\infty$, allora essa può essere iniettiva se e solo se è anche suriettiva.
- Dunque, essendo $|\mathbb{Z}_{a_1} \times ... \times \mathbb{Z}_{a_n}| = |\mathbb{Z}_m|$ ed essendo φ una funzione iniettiva, allora essa deve essere obbligatoriamente anche suriettiva.
- Concludiamo quindi che $\exists x \ \texttt{mod m} \in \mathbb{Z}_m$, abbiamo che

$$\varphi(x \ \texttt{mod m}) = (b_1 \ \texttt{mod}\ \ a_1, ..., b_n \ \texttt{mod}\ \ a_n)$$

  equivale a dire che x è l'unica soluzione del sistema.

Esempi:

1. • Cerchiamo una soluzione per il seguente sistema:

$$\begin{cases} x \equiv 2(\mathtt{mod}\ 3) \\ x \equiv 3(\mathtt{mod}\ 5) \\ x \equiv 2(\mathtt{mod}\ 7) \end{cases}$$

- Utilizzando la definizione di divisione con resto euclidea, $x \equiv 2(\mathtt{mod}\ 3)$ corrisponde ad affermare che $x = 2 + 3a, \forall a \in \mathbb{Z}$ (in modulo 3)
- Sostituendo $x = 2 + 3a$ dentro $x \equiv 3(\mathtt{mod}\ 5)$, otteniamo che:

$$2 + 3a \equiv 3(\mathtt{mod}\ 5)$$

- Applicando la definizione di relazione di congruenza, impostiamo l'equazione (dove le classi di congruenza sono descritte appartengono tutte a $\mathbb{Z}_5$):

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

- Applicando inversamente la definizione di relazione di congruenza, otteniamo quindi che $[a] = [2] \implies a \equiv 2(\mathtt{mod}\ 5) \implies a = 2 + 5b, \forall b \in \mathbb{Z}$
- Sostituendo $x = 2 + 3(2 + 5b) = 8 + 15b$ dentro $x \equiv 2(\mathtt{mod}\ 7)$, otteniamo che:

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

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

$$[8 + 15b] = [2]$$
$$[8] + [15][b] = [2]$$
$$[15][b] = [2] - [8]$$
$$[1][b] = [2] - [1]$$
$$[b] = [1]$$

- Quindi abbiamo che $[b] = [1] \implies b \equiv 1(\mathtt{mod}\ 7) \implies b = 1 + 7c, \forall c \in \mathbb{Z}$
- Infine, otteniamo che

$$x = 8 + 15(1 + 7c) = 23 + 105c, \forall c \in \mathbb{Z} \implies x \equiv 23(\mathtt{mod}\ 105)$$

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

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

2. • Cerchiamo una soluzione per il seguente sistema:

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

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

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

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

- Il nuovo sistema sarà quindi:

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

- Notiamo come la seconda e la quarta relazione di congruenza risultino in un'**incompatibilità del sistema**, poiché $1(\mathsf{mod}\ 5) \not\equiv 4(\mathsf{mod}\ 5)$, dunque **il sistema non può avere soluzioni**

3. • Cerchiamo una soluzione per il seguente sistema:

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

- Scomponendo in fattori primi si ha che:

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

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

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

- Il nuovo sistema sarà quindi:

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

- Abbiamo quindi che $x \equiv 0(\mathsf{mod}\ 3) \implies x = 0 + 3a, \forall a \in \mathbb{Z}$. Sostituendo nella seconda congruenza, otteniamo che $3a \equiv 1(\mathsf{mod}\ 5)$. Lavorando in $\mathbb{Z}_5$ quindi si ha che:

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

- Dunque $[a] = [2] \implies a \equiv 2(\mathsf{mod}\ 5) \implies a = 2 + 5b, \forall b \in \mathbb{Z}$.
- Sostituendo nella terza congruenza otteniamo $x = 3(2 + 5b) = 6 + 15b \implies 6 + 15b \equiv 3(\mathsf{mod}\ 4)$. Lavorando in $\mathbb{Z}_4$ quindi si ha che:

$$[6 + 15b] = [3]$$
$$[6] + [15][b] = [3]$$
$$[2] + [3][b] = [3]$$
$$[3][b] = [3] - [2]$$
$$[b] = [1][3]^{-1}$$
$$[b] = [3]$$

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

$$[51 + 60c] = [1]$$
$$[2] + [4][c] = [1]$$
$$[2] + [4][c] = [1]$$
$$[4][c] = [1] - [2]$$

$$[4][c] = [-1]$$
$$[c] = [6][4]^{-1}$$
$$[c] = [6][2]$$
$$[c] = [12]$$
$$[c] = [5]$$

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

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

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

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

4.
- Vogliamo calcolare le ultime due cifre di 37^{37}. Poniamo quindi $x := 37^{37}$ e calcoliamo la classe di equivalenza $x \ \mathtt{mod}\ 100$.
- 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 $\mathbb{Z}_{25}$

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

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

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

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

$$[1] + [4][k] = [17]$$
$$[4][k] = [16]$$
$$[k] = [16][4]^{-1}$$

$$[k] = [16][19]$$
$$[k] = [304]$$
$$[k] = [4]$$

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

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

  $$x \equiv y(\mathtt{mod}\ n) \implies y - x \in I(n) = y - x = n \cdot N = d(kN) \implies x \equiv y(\mathtt{mod}\ d)$$

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

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

- Riduciamo le classi di equivalenza del sistema:
  - Riduciamo $193x \equiv 1(\mathtt{mod}\ 3)$ in:

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

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

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

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

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

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

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

- Quindi si ha che $x = 1 + 16k \implies 1 + 16k \equiv 1(\mathtt{mod}\ 3)$:

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

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

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

- Infine $j = 2 + 5h \implies x = 1 + 48(2 + 5h) = 97 + 240h \implies x \equiv 97 (\mathtt{mod}\ 240)$
- Infatti in $\mathbb{Z}_{240}$ si ha che $[193][97] = [1]$

4.7 Piccolo teorema di Fermat

Prima di enunciare e dimostrare il teorema, affermiamo il seguenti due lemmi:

Lemma 18

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

$$p \left| \binom{p}{k} \right.$$

Dimostrazione:

- Dato che per sua definizione stessa il calcolo del coefficiente binomiale corrisponde ad un numero intero (si consiglia di leggere questa dimostrazione), il numeratore e il denominatore si semplificano tra di loro, tuttavia senza mai semplificare p, poiché esso è primo e i valori al denominatore sono minori di esso.

  Di conseguenza, si ha che:

$$\binom{p}{k} = n \cdot p, \exists n \in \mathbb{Z} \implies p \left| \binom{p}{k} \right.$$

  Esempio:

$$\binom{7}{3} = \frac{7!}{3! \cdot 4!} = \frac{7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2}{3 \cdot 2 \cdot 4 \cdot 3 \cdot 2} = 7 \cdot 5 \implies 7 \left| \binom{7}{3} \right.$$

Da tale lemma, quindi, traiamo che in $\mathbb{Z}_p$ si ha:

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

Inoltre, possiamo generalizzare tale casistica del caso in cui dato $n \in \mathbb{Z}$ dove $p \mid n$, in $\mathbb{Z}_p$ si ha:

$$n \cdot [a] = 0$$

Difatti, dato $p \mid n$, poiché siamo in $\mathbb{Z}_p$ si ha che:

$$n \cdot [a] = [na] = [pka] = [0]$$

Lemma 19

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:

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

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

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

- Se invece $0 < k < p$, per il lemma precedente sappiamo che in $\mathbb{Z}_p$:

$$p \left| \binom{p}{k} \right. \implies \binom{p}{k} \cdot [a] = 0$$

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

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

$$= \binom{p}{0}[b]^p + [0] + \ldots + [0] + \binom{p}{p}[a]^p = [b]^p + [a]^p$$

Tale lemma, inoltre, può essere esteso a n fattori:

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

Dimostrazione:

- Caso base (n=1):

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

- Caso base (n=2): coincide con il lemma appena enunciato
- Passo induttivo:

$$([a_1]+\ldots+[a_n]+[a_{n+1}])^p = ([[a_1]+\ldots+[a_n]]+[a_{n+1}])^p = ([a_1]+\ldots+[a_n])^p+[a_{n+1}]^p =$$

$$= ([a_1] + \ldots + [a_{n-1}])^p + [a_n]^p + [a_{n+1}]^p = \ldots\ldots = [a_1]^p + \ldots + [a_{n+1}]^p$$

Theorem 20. Piccolo teorema di Fermat

In $\mathbb{Z}_p$ si ha che $\forall p \in \mathbb{P}, \forall a \in \mathbb{Z}$ vale:

$$a^p \equiv a(\texttt{mod}\ p)$$

Dimostrazione:

- Caso base (a=0):
$$[0]^p = [0]$$
- Ipotesi induttiva:
$$[a]^p = [a]$$
- Passo induttivo:
$$[a+1]^p = ([a]+[1])^p = [a]^p + [1]^p = [a]^p + [1] = [a] + [1] = [a+1]$$

Tramite tale teorema, inoltre, possiamo dimostrare che:

$$[a]^p = [a]$$
$$[a]^k[a]^p = [a][a]^k$$
$$[a]^{p+k} = [a][a]^{k+1-1}$$
$$[a]^{p+k} = [a][a]^{-1}[a]^{k+1}$$
$$[a]^{p+k} = [1][a]^{k+1}$$
$$[a]^{p+k} = [a]^{k+1}$$

Ad esempio, abbiamo che $a^{p-2} \equiv a^{-1}(\texttt{mod}\ p)$ e che $5^7 \equiv 5^5 \equiv 5^3 \equiv 5 \equiv 2(\texttt{mod}\ 3)$.

4.8 Ordine di un elemento di un gruppo

Definition 34. Sottogruppo ciclico e ideale d'ordine

Sia G un gruppo e sia $g \in G$. Definiamo il sottogruppo $H(g) \subseteq G$ (detto **sottogruppo ciclico**) e l'ideale $I(g) \subseteq \mathbb{Z}$ come:

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

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

Dimostrazione:

- $(H(g), \cdot) \subseteq (G, \cdot)$
  - $g^0 = e \implies e \in H(g)$

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

Definition 35. Ordine di un elemento di un gruppo

Sia G un gruppo e sia $g \in G$. Dato $H(g) : \{g^n \mid n \in \mathbb{Z}\}$, definiamo l'**ordine di** g come:

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

Proposition 21

Dato $g \in G$ e dato l'ideale $I(g) : \{n \in \mathbb{Z} \mid g^n = e\}$, poiché $\mathbb{Z}$ è un dominio a ideali principali, allora $\exists! d \geq 0 \mid I(g) = I(d)$ dove:

- $d = 0 \implies o(g) = \mathbb{Z} = " + \infty"$
- $d > 0 \implies o(g) = d$

dunque $o(g) = d := |H(g)|$ corrisponde al **più piccolo esponente** tale che $g^d = e$

Dimostrazione:

- Supponendo $I(g) = I(d)$, abbiamo che:

$$n, m \in I(g) \implies g^n = g^m \implies g^{-n} \cdot g^n = g^m \cdot g^{-n} \implies e = g^{m-n} \implies$$
$$\implies m - n \in I(g) = I(d) \implies d \mid m - n$$

- Se $d = 0$, si ha:
  - Siccome $d \mid m - n$, allora
  $$0 \mid m - n \implies m - n = 0 \implies m = n$$
  concludendo che $n \neq m \implies g^n \neq g^m$
  - Di conseguenza, la funzione descrivente il sottogruppo $H(g)$
  $$f : \mathbb{Z} \to H(g) : n \mapsto g^n$$
  è biettiva, associando quindi ogni $n \in \mathbb{Z}$ ad un diverso $g^n \in H(g)$.
  - Tuttavia, poiché $|\mathbb{Z}| = " + \infty"$, ne segue che anche $|H(g)| = " + \infty"$ affinché la funzione possa rimanere biettiva, implicando quindi che:
  $$o(g) := |H(g)| = |\mathbb{Z}| = " + \infty"$$

- Se invece $d > 0$, si ha:
  - Poiché $I(g) = I(d) \implies g^d = e$, esiste $n \in \mathbb{Z}$ divisibile con resto per d tale che:

    $$n = qd + r, \exists q, r \in \mathbb{Z}, 0 \leq r < d \implies g^n = g^{qd+r} = (g^d)^q \cdot g^r = e^q \cdot g^r = g^r$$

    poiché $0 \leq r < d$, concludiamo che $H(g)$ possa contenere al massimo d elementi, dunque $o(g) := |H(g)| \leq d$
  - Mostriamo ora che presi $0 \leq m, n < d \implies -d < m - n < d$, si ha che

    $$g^n = g^m \implies g^{m-n} = e \implies g^{m-n} = (g^d)^k, \forall k \in \mathbb{Z} \implies$$
    $$\implies g^{m-n} = g^{dk} \implies m - n = dk \implies d \mid m - n$$

  - L'unico numero $-d < m-n < d$ tale che $m-n = dk, \exists k \in \mathbb{Z}$ è 0, di conseguenza $m - n = 0 \implies m = n$, implicando quindi che

    $$H(g) : \{e = x^0 \mid x \in \{g^0 ..., g^{d-1}\}\} = \{g^0 ..., g^{d-1}\}$$

    e di conseguenza che $o(g) := |H(g)| = d$

Proposition 22

Se G è un gruppo con cardinalità finita, allora per $g \in G$ si ha che

$$o(g) := |H(g)| \leq |G| < +\infty$$

Dunque, per il **teorema di Lagrange** si ha che:

$$o(g) \mid |G| \implies g^{|G|} = e$$

Attenzione: $o(g) \mid |G| \iff o(g) < +\infty$

Dimostrazione:

- Dato $o(g) = d := |H(g)|$, allora

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

Inoltre, tramite tale proposizione possiamo trovare una **seconda dimostrazione del piccolo teorema di Fermat**:

2° Dimostrazione del PTF:

- Se $[a] = [0]$, allora abbiamo che $[a]^p = [0]$
- Se $[a] \neq [0]$, ricordiamo che $\mathbb{Z}_p$ corrisponde ad un campo, dunque si ha che $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$, implicando che $\left|\mathbb{Z}_p^*\right| = p - 1$.
- Di conseguenza, per via della proposizione precedente, dato $[a] \in \mathbb{Z}_p^*$ si ha che:

  $$[a]^{\left|\mathbb{Z}_p^*\right|} = [1] \implies [a]^{p-1} = [1] \implies [a]^p [a]^{-1} = [1] \implies [a]^p = [a]$$

Proposition 23. Gruppo ciclico

Dato un gruppo finito G e $g \in G$, siccome $H(g) \subseteq G$, allora

$$o(g) := |H(g)| = |G| < +\infty \iff G = H(g)$$

In tal caso definiamo G come **gruppo ciclico**

Observation 17

Dato un gruppo G e $g \in G$, se g è invertibile allora

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

Lemma 24

Dato un gruppo G e $g \in G$ se g è invertibile allora

$$|H(g)| =: o(g) = o(g^{-1}) := \left|H(g^{-1})\right|$$

Dimostrazione:

- Basta osservare che $(g^{-1})^n = g^{-n}$ e $g^n = (g^{-1})^{-n}$ per ogni $n \in \mathbb{Z}$, dunque ogni potenza di g è anche una potenza di g^{-1} e viceversa
- Di conseguenza, si verifica che $H(g) = H^{-g}$, implicando quindi che $o(g) = o(g^{-1})$

Lemma 25

Dato G un gruppo finito e $k \in \mathbb{Z}$, per ogni $g \in G$ si verifica che:

$$o(g^k) \mid o(g)$$

Dimostrazione:

- Basta osservare che $(g^k)^n = g^{nk}$, dunque ogni potenza di g^k è anche una potenza di g. Di conseguenza, si verifica che $H(g^k) \subseteq H(g)$. Poiché H è un sottogruppo finito, allora per Lagrange abbiamo che $o(g^k) := \left|H(g^k)\right| \mid |H(g)| =: o(g)$

Lemma 26

Dato G un gruppo finito e $g, h \in G \mid gh = hg$, posti $m := mcm(o(g), o(h))$ e $d := MCD(o(g), o(h)$ si ha che

$$\frac{m}{d} \mid o(gh) \qquad \text{e} \qquad o(gh) \mid m$$

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

Dimostrazione:

- Siano $a := o(g)$ e $b := o(h)$. Per definizione stessa si ha che m è multiplo sia di a che di b, dunque $m = ap = bq, \exists p, q \in \mathbb{Z}$.
- Siccome per ipotesi abbiamo che $gh = hg$ e siccome $c := o(g)$ è il più esponente per cui $(gh)^c = e$, abbiamo che

$$(gh)^m = g^m h^m = g^{ap} h^{bq} = (g^a)^p (h^b)^p = e^p e^q = e \implies c := o(gh) \mid m$$

- Viceversa, abbiamo che

$$e = (gh)^c = g^c h^c \implies e = g^c h^c \implies k := g^c = h^- c$$

- Siccome per il lemma precedente $o(k) = o(g^c) \mid o(g)$ e $o(k) = o(h^{-c}) \mid o(h)$, allora $o(k) \mid d$, implicando che:

$$\frac{m}{d} \mid \left(\frac{m}{d} \cdot \frac{d}{o(k)} \right) = \frac{m}{o(k)}$$

- Inoltre, abbiamo che

$$g^{o(k)c} = (g^c)^{o(k)} = k^{o(k)} = e \implies a := o(g) \mid o(k)c$$

  e analogamente che:

$$h^{-o(k)c} = (h^{-c})^{o(k)} = k^{o(k)} = e \implies b : o(h) \mid -o(k)c \implies b \mid o(k)c$$

  di conseguenza si ha che $m \mid o(k)c$

- Quindi, $\exists j \in \mathbb{Z}$ tale che:

$$o(k)c = mj \implies c = \frac{m}{o(k)} \cdot j \implies \frac{m}{o(k)} \mid c := o(gh)$$

- Infine, per transitività si ha che:

$$\frac{m}{d} \mid \frac{m}{o(k)} \wedge \frac{m}{o(k)} \mid o(gh) \implies \frac{m}{d} \mid o(gh)$$

- Per l'ultima affermazione notiamo che se $d = 1$, allora per il teorema fondamentale dell'aritmetica si ha $m = o(g)o(h)$. Avendo già mostrato che:

$$\frac{m}{d} \mid o(gh)$$

  e che

$$o(gh) \mid m$$

  se $d = 1$ allora

$$m \mid o(gh) \wedge o(gh) \mid m \iff o(gh) = m = o(g)o(h)$$

Esempio:

- Vogliamo trovare tutti gli inversi di $\mathbb{Z}_{21}$ e il loro ordine, determinando se $\mathbb{Z}_{21}$ sia un gruppo ciclico
- Dato $g \in \mathbb{Z}_{21}$, sappiamo che $g \in \mathbb{Z}_{21}^* \iff MCD(a, 21) = 1$ (sezione 4.4). 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:

$$o(g) \mid |\mathbb{Z}_{21}^*| \implies o(g) \mid 12 \implies o(g) = \begin{cases} 1 \\ 2 \\ 3 \\ 4 \\ 6 \\ 12 \end{cases}$$

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

Proposition 27

Siano $n_1, \ldots, n_k \neq 0 \in \mathbb{N}$ dove $MCD(a_i, a_j) \iff i \neq j$. Per il teorema fondamentale dell'aritmetica, si ha $N := mcm(n_1, \ldots, n_k) = n_1 \cdot \ldots \cdot \cdots \cdot n_k$.

Dato $[a] \in \mathbb{Z}^*_{\gtrdot}$, sia o l'ordine di $[a]$ in nel gruppo $\mathbb{Z}^*_{\gtrdot}$ e sia o_h l'ordine di $[a]$ nel gruppo $\mathbb{Z}^*_{\ltimes_{\widetilde{>}}}, \forall 0 < h < k$.

In tal caso, si ha che:

$$o = m := mcm(o_1, \ldots, o_k)$$

Dimostrazione:

- Per il teorema cinese dei resti, abbiamo che:

$$a^o \equiv 1(\texttt{mod}\ \ N) \iff \begin{cases} a^o \equiv 1(\texttt{mod}\ \ n_1) \\ \vdots \\ a^o \equiv 1(\texttt{mod}\ \ n_k) \end{cases} \iff$$

$$\iff \begin{cases} o_1 \mid o \\ \vdots \\ o_k \mid o \end{cases} \iff m := mcm(o_1, \ldots, o_k) \mid o$$

- Inoltre, poiché $m := mcm(o_1, \ldots, o_k)$, abbiamo che:

$$\begin{cases} o_1 \mid m \\ \vdots \\ o_k \mid m \end{cases} \iff \begin{cases} a^m \equiv 1(\texttt{mod}\ \ n_1) \\ \vdots \\ a^m \equiv 1(\texttt{mod}\ \ n_k) \end{cases} \iff a^m \equiv 1(\texttt{mod} N) \implies o \mid m$$

- Siccome $o \mid m$ e $m \mid o$, l'unica possibilità è che $o = m$

Capitolo 5

Gruppo Simmetrico

Definition 36. Gruppo simmetrico

Dato un insieme X, denotiamo come $\mathbb{S}_X$ l'insieme composto da tutte le funzioni biettive da X in se stesso.

$$\mathbb{S}_X : \{f : X \to X \mid f \texttt{ è biettiva}\}$$

Inoltre, si ha che $(\mathbb{S}_X, \circ)$ è un gruppo.

Dimostrazione:

- $f, g, h \in \mathbb{S}_X \implies h \circ (g \circ f) = h \circ h \circ f = (h \circ g) \circ f$
- $\exists \texttt{id} : x \mapsto x \in \mathbb{S}_X \mid \forall f \in \mathbb{S}_X, f \circ \texttt{id} = \texttt{id} \circ f = f$
- $\exists f^{-1} : f(x) \mapsto x \in \mathbb{S}_X \mid f \circ f^{-1} = f^{-1} \circ f = \texttt{id}$

Observation 18

Una funzione f può essere invertibile se e solo se f è biettiva.

$$f \texttt{ è invertibile} \iff f \texttt{ è biettiva}$$

Dimostrazione:

- Se f è invertibile, allora:
  - f è suriettiva poiché $x = f(f^{-1}(x)), \forall x \in X$
  - f è iniettiva poiché $f(x) = f(y) \implies x = f^{-1}(f(x)) = f^{-1}(f(y)) = y$
- Se f è biettiva, allora $\forall x \in X, \exists! y \mid f(y) = x$

  Ponendo $y = f^{-1}(x)$, il vincolo biettivo è rispettato e inoltre otteniamo che

$$\forall f \in S_X, \exists f^{-1} \in S_X \mid f \circ f^{-1} = f^{-1} \circ f$$

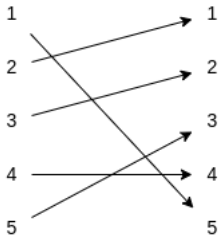
Il gruppo simmetrico presenta alcune **caratteristiche**:

- Trattandosi di funzioni biettive, ogni elemento del gruppo simmetrico corrisponde ad una **permutazione** del dominio X
- Se X è finito, ossia possiede un numero finito di elementi (dunque $|X| = n$), allora denotiamo il suo **gruppo simmetrico di ordine** n come $\mathcal{S}_n$
- Poiché **tutte le permutazioni possibili** di un insieme di n elementi corrispondono a $n!$, allora abbiamo che $|X| = n \implies |\mathcal{S}_n| = n!$

Data una **permutazione** $\sigma \in \mathcal{S}_n$, possiamo utilizzare due notazioni per poterne descrivere il comportamento:

Tramite grafo

σ



Tramite matrice

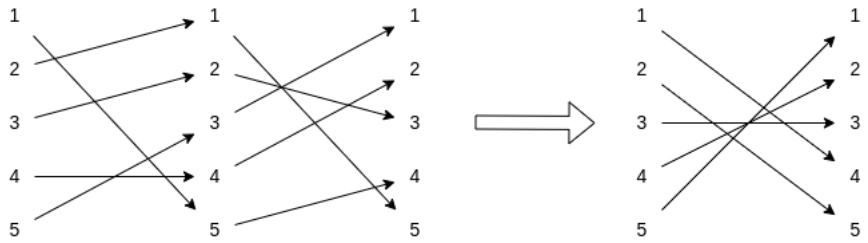
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix}$$

Definiamo l'operazione **prodotto tra due permutazioni** come la **composizione di due funzioni**, dunque $\tau\sigma = \tau(\sigma)$.

Quindi si ha che:

- Per effettuare il prodotto tramite rappresentazione con grafo, ci basta considerare l'**unione delle frecce** appartenenti ad ognuna delle permutazioni:

σ **τ** **τσ**



- Per effettuare il prodotto tramite rappresentazione con matrici, ci basta far "scorrere" gli elementi iniziali della seconda permutazione affinché coincidano con quelli finali della prima permutazione. Il risultato del prodotto sarà costituito dagli **elementi iniziali della prima** (o sia il fattore destro) e gli **elementi finali della seconda** (ossia il fattore sinistro):

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

Observation 19

Poiché il prodotto è dato dalla composizione, tale operazione non è commutativa, dunque

$$\tau\sigma \neq \sigma\tau$$

5.1 Ordine di una permutazione

Un caso particolare di ordine di un elemento appartenente ad un gruppo è quello delle **permutazioni**.

Definition 37. Ciclo di una permutazione

Data $\sigma \in \mathcal{S}_n$, definiamo come **ciclo di** σ una sequenza di interi $1 \leq i_1, ..., i_n \leq n$ tutti distinti tra loro tali che:

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, ..., \sigma(i_n) = i_1$$

Definiamo come **lunghezza del ciclo** il numero di elementi appartenenti al ciclo.

Ad esempio, consideriamo la seguente permutazione in 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:

- $1 \to 5 \to 2 \to 7 \to 1$ che abbreviamo come (1587)
- $3 \to 6 \to 3$ che abbreviamo come (36)
- $4 \to 9 \to 8 \to 4$ che abbreviamo come (498)

Nel nostro esempio, quindi, abbiamo tre cicli di lunghezza rispettiva 4, 2 e 3, i quali descrivono la permutazione stessa $\sigma = (1587)(36)(498)$

Definition 38. Decomposizione in cicli

Data $\sigma \in \mathcal{S}_n$ composta da k cicli, definiamo la sua **decomposizione in cicli** come:

$$\sigma = \gamma_1\gamma_2 \dots \gamma_k$$

dove γ_i è un ciclo di σ

Notiamo, inoltre, la possibilità di **ricostruire una permutazione** qualsiasi tramite la sua decomposizione in cicli. Ad esempio, in S_8 si ha che:

$$\sigma = (235)(1874)(6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 5 & 1 & 2 & 6 & 4 & 7 \end{pmatrix}$$

Definition 39

Data $\sigma \in \mathcal{S}_n$ e dato $1 \leq i \leq n$, definiamo i seguenti due ideali di $(\mathbb{Z}, +)$:

$$I(\sigma, i) : \{n \in \mathbb{Z} \mid \sigma^n(i) = i\}$$

$$I(\sigma) : \{n \in \mathbb{Z} \mid \sigma^n = \mathtt{id}\}$$

dove `id` rappresenta la **permutazione identica**, ossia quella che manda ogni elemento in se stesso, corrispondente quindi all'elemento neutro in $\mathcal{S}_n$.

Dimostriamo quindi che si tratta di due ideali (la dimostrazione per il secondo ideale è analoga a quella del primo, dunque verrà omessa):

- $\sigma^0(i) = \mathtt{id}(i) = i \implies 0 \in I(\sigma, i)$
- $m, n \in I(\sigma, i) \implies \sigma^n(i) = \sigma^n(i) = i \implies \sigma^{n+m}(i) = (\sigma^n)^m(i) = \sigma^m(i) = i \implies m + n \in I(\sigma, i)$
- $n \in I(\sigma, i) \implies \sigma^{-n}(i) = (\sigma^n)^{-1}(i) = i \implies -n \in I(\sigma, i)$
- $n \in I(\sigma, i) \implies \sigma^{nk}(i) = (\sigma^n)^k(i) = i, \forall k \in \mathbb{Z} \implies nk \in I(\sigma, i), \forall k \in \mathbb{Z}$

Per gli ultimi due punti è necessario osservare che data una permutazione $\sigma \in \mathcal{S}_n$ dove $\sigma(i) = i$, dunque i viene sempre mandato in se stesso, allora $\sigma^k(i) = i, \forall k \in \mathbb{Z}$.

Lemma 28

Se $i \leq i \leq n$ è un elemento appartenente ad un ciclo di σ di lunghezza d, poiché $\mathbb{Z}$ è un dominio ad ideali principali si ha che $I(\sigma, i) = I(d)$

Dimostrazione:

- Ci basta verificare che se $d \in I(\sigma, i)$ e $0 < k < d$, allora $k \notin I(\sigma, i)$.
- Sia quindi $i \in (i_1 i_2 ... i_d)$, ossia appartenente ad un ciclo di lunghezza d. Per comodità, supponiamo che $i = i_1$, poiché scorrere l'ordine degli elementi del ciclo non ne cambia le proprietà (ad esempio: $(2783) = (7832)$)
- Si verifica quindi che:

$$0 < k < d \implies \sigma^k(i) = \sigma(\sigma^{k-1}(i)) = \sigma(i_k) = i_{k+1}$$

- Nel caso in cui invece $k = d$, si verifica che:

$$k = d \implies \sigma^d(i) = \sigma(i_d) = i_1$$

- Di conseguenza, **la più piccola potenza di σ che manda i in se stesso è** d, dove d è la lunghezza del ciclo.

Lemma 29. Ordine di una permutazione

Data $\sigma \in \mathcal{S}_n$ e data la sua decomposizione in cicli $\sigma = \gamma_1\gamma_2...\gamma_k$, si verifica che

$$o(\sigma) = mcm(d_1, ..., d_k)$$

dove d_i è la lunghezza del ciclo γ_i

Dimostrazione:

- Per definizione stessa dei due ideali $I(\sigma)$ e $I(\sigma, i)$, si ha che:

$$n \in I(\sigma) \iff \sigma^n = \texttt{id} \iff \sigma^n(i) = i, \forall 1 \leq i \leq n \iff$$
$$\iff n \in I(\sigma, i), \forall 1 \leq i \leq n \iff n \in I(\sigma, 1) \cap ... \cap I(\sigma, n)$$

- Di conseguenza, dato $d := o(\sigma)$ e $m := mcm(d_1, ..., d_n))$, per via delle proprietà degli ideali si verifica che:

$$I(d) = I(\sigma) = I(\sigma, 1) \cap ... \cap I(\sigma, n) = I(d_1) \cap ... \cap I(d_n) = I(m)$$

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:

$$o(\sigma) = mcm(5, 2) = 10$$

- Data $\sigma \in S_{15}$ tale che:

$$\sigma = (1\ 2\ 10\ 8\ 3)(11\ 7)(4\ 12\ 14\ 6)(13)(5\ 15\ 9)$$

  L'ordine di tale permutazione risulta essere:

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

5.2 Segno delle permutazioni

Definition 40

Data $\sigma \in \mathcal{S}_n$, definiamo come **inversione di** σ una coppia di valori (i, j) dove $1 \leq i, j \leq n$ tale che $\sigma(i) > \sigma(j)$.

Denotiamo quindi l'insieme delle inversioni di σ come:

$$Inv(\sigma) : \{1 \leq i, j \leq n \mid \sigma(i) > \sigma(j)\}$$

Ad esempio, data la permutazione

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

l'insieme delle sue inversioni sarà:

$$Inv(\sigma) : \{(1,4),(2,3),(2,4),(2,5),(3,4)\}$$

Definiamo quindi il **segno di** σ come:

Definition 41. Segno di una permutazione

Data $\sigma \in \mathcal{S}_n$ e dato l'insieme delle sue inversioni definito come

$$Inv(\sigma) : \{1 \leq i, j \leq n \mid \sigma(i) > \sigma(j)\}$$

il **segno della permutazione** σ corrisponde a:

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

Affermiamo che σ è **pari** se il suo segno è $+1$, mentre è **dispari** se il suo segno è -1.

Definition 42

Dati $1 \leq i < j \leq n$, definiamo come **trasposizione** un particolare tipo di permutazione $\tau_{i,j} \in \mathcal{S}_n$ tale che:

$$\tau_{i,j}(k) = \begin{cases} j & \text{se } k = i \\ i & \text{se } k = j \\ k & \text{se } k \neq i \wedge k \neq j \end{cases}$$

In particolare, definiamo come **trasposizione adiacente** una trasposizione in cui $j = i + 1$, dunque del tipo $\tau_{i,i+1}$, scambiando quindi due elementi adiacenti tra loro.

Lemma 30

Data una permutazione $\sigma \in \mathcal{S}_n$, essa può essere espressa come il **prodotto di** k **trasposizioni adiacenti**:

$$\exists 1 \leq i_1, ..., i_k \mid \sigma = \tau_{i_1,i_1+1} \cdot ... \cdot \tau_{i_k,i_k+1}$$

Dimostrazione tramite esempio:

- Osserviamo prima come dati $\sigma, \tau_{i,j} \in \mathcal{S}_n$, quindi definiti come:

$$\sigma = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ \sigma(1) & \dots & \sigma(i) & \dots & \sigma(j) & \dots & \sigma(n) \end{pmatrix}$$

$$\tau_{i,j} = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ 1 & \dots & j & \dots & i & \dots & n \end{pmatrix}$$

  si ha che:

$$\sigma\tau_{i,j} = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ \sigma(1) & \dots & \sigma(j) & \dots & \sigma(i) & \dots & \sigma(n) \end{pmatrix}$$

- Ad esempio, quindi, Data $\sigma \in S_3$ definito come:

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

  abbiamo che:

$$\sigma \cdot \tau_{3,4} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \implies \sigma \cdot \tau_{3,4} \cdot \tau_{2,3} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \implies$$

$$\implies \sigma \cdot \tau_{3,4} \cdot \tau_{2,3} \cdot \tau_{1,2} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \implies \sigma \cdot \tau_{3,4} \cdot \tau_{2,3} \cdot \tau_{1,2} \cdot \tau_{3,4} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \mathtt{id}$$

- Dunque, si ha che:

$$\sigma(\tau_{3,4}\tau_{2,3}\tau_{1,2}\tau_{3,4}) = \mathtt{id}$$
$$\sigma(\tau_{3,4}\tau_{2,3}\tau_{1,2}\tau_{3,4})(\tau_{3,4}\tau_{2,3}\tau_{1,2}\tau_{3,4})^{-1} = \mathtt{id}(\tau_{3,4}\tau_{2,3}\tau_{1,2}\tau_{3,4})^{-1}$$
$$\sigma = (\tau_{3,4}\tau_{2,3}\tau_{1,2}\tau_{3,4})^{-1}$$
$$\sigma = \tau_{3,4}\tau_{1,2}\tau_{2,3}\tau_{3,4}$$

Proposition 31

Data $\sigma \in \mathcal{S}_n$ dove $\sigma = \tau_1 \cdot \dots \cdot \tau_k$ dove $\tau_i = \tau_{i,i+1} \in \mathcal{S}_n$ (ossia sono trasposizioni adiacenti), allora si ha che:

$$sgn(\sigma) = (-1)^k$$

dove k è il numero di trasposizioni adiacenti che compongono σ

Dimostrazione:

- Sia $\tau = \tau_{i,i+1}$. Allora si ha che:

$$\sigma\tau = \begin{pmatrix} 1 & \dots & i & i+1 & \dots & n \\ \sigma(1) & \dots & \sigma(i+1) & \sigma(i) & \dots & \sigma(n) \end{pmatrix}$$

- Lo scambio effettuato genera una di due situazioni: viene **creata una nuova inversione** oppure viene **risolta un'inversione pre-esistente**:

$$Inv(\sigma\tau) = \begin{cases} Inv(\sigma) \cup \{(i, i+1)\} & \text{se } (i, i+1) \notin Inv(\sigma) \\ Inv(\sigma) \setminus \{(i, i+1)\} & \text{se } (i, i+1) \in Inv(\sigma) \end{cases}$$

- Di conseguenza, si verifica che

$$|Inv(\sigma\tau)| = |Inv(\sigma)| \pm 1$$

  dunque se $|Inv(\sigma)|$ è dispari allora $|Inv(\sigma\tau)|$ sarà pari, mentre se $|Inv(\sigma)|$ è pari allora $|Inv(\sigma\tau)|$ sarà dispari. Quindi, si verifica che:

$$sgn(\sigma\tau) = -sgn(\sigma)$$

- Data $\sigma = \tau_i \cdot ... \cdot \tau_k$, si ha che:

$$\sigma(\tau_i \cdot ... \cdot \tau_k)^{-1} = (\tau_i \cdot ... \cdot \tau_k)(\tau_i \cdot ... \cdot \tau_k)^{-1} = \texttt{id}$$

- Poiché `id` non ha alcuna inversione per sua definizione stessa, si ha che $sgn(\texttt{id}) = 1$. Di conseguenza, si verifica che:

$$1 = sgn(\texttt{id}) = sgn(\sigma(\tau_i \cdot \tau_2 \cdot \tau_3 \cdot ... \cdot \tau_k)^{-1}) = sgn(\sigma \cdot \tau_k \cdot ... \cdot \tau_3 \cdot \tau_2 \cdot \tau_1) =$$

$$= -sgn(\sigma \cdot \tau_k \cdot ... \cdot \tau_3 \cdot \tau_2) = sgn(\sigma \cdot \tau_k \cdot ... \cdot \tau_3) = ... = (-1)^k \cdot sgn(\sigma)$$

- Quindi, affermiamo che:

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

Corollary 8

Date due permutazioni $\sigma, \sigma' \in \mathcal{S}_n$, si verifica che:

$$sgn(\sigma\sigma') = sgn(\sigma) \cdot sgn(\sigma')$$

Dimostrazione:

- Data $\sigma = \tau_1 \cdot ... \cdot \tau_k$ e $\sigma' = \tau'_1 \cdot ... \cdot \tau'_k$, si ha che:

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

Corollary 9

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

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

Dimostrazione:

- Poiché
$$1 = sgn(\mathtt{id}) = sgn(\sigma\sigma^{-1}) = sgn(\sigma) \cdot sgn(\sigma^{-1})$$
allora si ha che:
$$1 = sgn(\sigma) \cdot sgn(\sigma^{-1}) \implies sgn(\sigma) = sgn(\sigma^{-1})$$

Definition 43

Denotiamo il sottogruppo $A_n \subseteq \mathcal{S}_n$ come **gruppo alterno di ordine** n, definito come:
$$A_n := \{\sigma \in \mathcal{S}_n \mid sgn(\sigma) = +1\}$$

Data la relazione che σ e σ' sono nella stessa classe laterale sinistra se e solo se
$$\sigma^{-1}\sigma' \in A_n \implies 1 = sgn(\sigma^{-1}\sigma') = sgn(\sigma^{-1}) \cdot sgn(\sigma') =$$
$$= sgn(\sigma) \cdot sgn(\sigma') \iff sgn(\sigma) = sgn(\sigma')$$

Notiamo come $\mathcal{S}_n$ venga partizionato in esattamente due classi laterali, una contente tutte le permutazioni pari (coincidente con A_n) ed una contenente tutte le dispari.

Dunque, per il teorema di Lagrange, si ha che:
$$2 = |\mathcal{S}_n/A_n| = \frac{|\mathcal{S}_n|}{|A_n|} \implies |A_n| = \frac{|\mathcal{S}_n|}{2} = \frac{n!}{2}$$

Vogliamo ora dimostrare che data $\sigma \in \mathcal{S}_n$ e data la sua scomposizione in cicli $\sigma = \gamma_1 ... \gamma_k$, si ha che $sgn(\sigma) = (-1)^{n-k}$.

Riprendiamo quindi la **relazione di coniugato** (sezione 3.5), ossia:
$$x \sim y \iff \exists a \in G \mid y = axa^{-1}$$

In particolare, nel **caso delle permutazioni**, dati $\sigma, \sigma' \in \mathcal{S}_n$ si ha che:
$$\exists \alpha \in \mathcal{S}_n \mid \sigma = \alpha\sigma\alpha^{-1} \implies sgn(\sigma') = sgn(\alpha) \cdot sgn(\sigma) \cdot sgn(\alpha^{-1})$$

Tuttavia, poiché $sgn(\alpha) = sgn(\alpha^{-1}) = \pm 1 \implies sgn(\alpha) \cdot sgn(\alpha^{-1}) = 1$, si ha che:
$$sgn(\sigma') = sgn(\alpha) \cdot sgn(\sigma) \cdot sgn(\alpha^{-1}) =$$
$$= \begin{cases} 1 \cdot sgn(\sigma) \cdot 1 & sgn(\alpha) = sgn(\alpha^{-1}) = 1 \\ (-1) \cdot sgn(\sigma) \cdot (-1) & sgn(\alpha) = sgn(\alpha^{-1}) = -1 \end{cases} = sgn(\sigma)$$

Proposition 32

Dati $\sigma, \sigma' \in \mathcal{S}_n$, date le loro scomposizioni in cicli $\sigma = \gamma_1 ... \gamma_k$ e $\sigma' = \gamma'_1 ... \gamma'_h$ e date le lunghezze dei loro cicli d_j e d'_j, supponendo $d_1 \leq ... \leq d_k$ e $d'_1 \leq ... \leq d'_h$ si ha che:

$$\sigma \sim \sigma' \iff \begin{cases} k = h \\ d_1 = d'_1 \\ ... \\ d_k = d'_h \end{cases}$$

Dimostrazione:

- Supponiamo che $\sigma \sim \sigma'$, dunque $\exists \alpha \in \mathcal{S}_n \mid \sigma' = \alpha\sigma\alpha^{-1}$
- Se $(i_1 ... i_d)$ è un ciclo di σ, allora $(\alpha(i_1) ... \alpha(i_d))$ è un ciclo di σ'. Difatti si ha che:

$$\sigma'\alpha(i_j) = \alpha\sigma\alpha^{-1}\alpha(i_j)) = \alpha\sigma(i_j) = \begin{cases} \alpha(i_{j+1}) & \text{se } j < d \\ \alpha(i_1) & \text{se } j = d \end{cases}$$

- Ciò stabilisce quindi una corrispondenza biunivoca tra i cicli di σ e quelli di σ' (dunque $h = k$), i quali inoltre avranno la stessa lunghezza (dunque $d_i = d'_i$)
- Siano quindi $\sigma = (i_1 ... i_{d_1}) ... (j_1 ... j_{d_2})$ e $\sigma' = (a_1 ... a_{d'_1}) ... (b_1 ... b_{d'_2})$
- Definiamo $\alpha \in \mathcal{S}_n \mid \alpha(i_k) = a_k, ..., \alpha(j_h) = b_h$
- Ad esempio, si avrà quindi che:

$$\alpha\sigma\alpha^{-1}(a_k) = \alpha\sigma(i_k) = \begin{cases} \alpha(i_{k+1}) & \text{se } k < d_1 \\ \alpha(i_1) & \text{se } k = d_1 \end{cases} = \begin{cases} a_{k+1} & \text{se } k < d_1 \\ a_1 & \text{se } k = d_1 \end{cases}$$

Esempi:

1. Date le seguenti permutazioni $\sigma, \sigma' \in S_6$, trovare $\alpha \in S_6$ tale che $\sigma' = \alpha\sigma\alpha^{-1} \implies \sigma' \sim \sigma$:

$$\begin{matrix} \sigma = (13)(254)(876) \\ \sigma' = (25)(184)(376) \end{matrix} \implies \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 5 & 4 & 8 & 6 & 7 & 3 \end{pmatrix}$$

2. Date le seguenti permutazioni $\sigma, \sigma' \in S_7$, trovare $\alpha \in S_7$ tale che $\sigma' = \alpha\sigma\alpha^{-1} \implies \sigma' \sim \sigma$:

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

Proposition 33

Data $\sigma \in \mathcal{S}_n$ e data la sua scomposizione in cicli $\sigma = \gamma_1 ... \gamma_k$, allora si ha che:

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

Dimostrazione:

- Supponiamo che $\exists \sigma' \in \mathcal{S}_n \mid \sigma' \sim \sigma$. Si ha quindi che:

$$\sigma = (i_1 \ ... \ i_{d_1})(i_{d_1+1} \ ... \ i_{d_2}) \ ... \ (j_1 \ ... \ j_{d_k})$$

$$\sigma' = (1 \ ... \ d_1)(d_1 + 1 \ ... \ d_1 + d_2) \ ... \ (n - d_k + 1 \ ... \ n)$$

- Di conseguenza, σ' corrisponderà a:

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

- Ricordando che $\sigma \sim \sigma' \implies sgn(\sigma') = sgn(\sigma)$, ci basterà trovare il segno di σ' per verificare la proposizione.
- Notiamo come affinché la permutazione mandi ogni elemento nel range $[1, d_1]$ (corrispondente al primo ciclo) in se stesso siano necessari $d_1 - 1$ trasposizioni adiacenti:

$$\sigma \cdot \tau_{d_1-1,d_1} \cdot \tau_{d_1-2,d_1-1} \cdot ... \cdot \tau_{2,3} \cdot \tau_{1,2} =$$

$$= \begin{pmatrix} 1 & 2 & ... & d_1 & d_1+1 & ... & d_1+d_2 & ... & ... & n-(d_k+1) & ... & n \\ 1 & 2 & ... & d_1 & d_1+2 & ... & d_1+1 & ... & ... & n-(d_k+1)+1 & ... & n-(d_k+1) \end{pmatrix}$$

- Analogamente, ogni altro range corrispondente al ciclo di lunghezza d_j di σ' necessiterà di $d_j - 1$ trasposizioni, in modo da ottenere la permutazione identica
- Di conseguenza, affermiamo che il numero di trasposizioni componenti σ' sia

$$\sum_{j=1}^{k} d_j - 1$$

  dove k ricordiamo essere il numero di cicli della decomposizione di σ'.
- Poiché la somma di tutte le lunghezze dei cicli per definizione stessa corrisponde ad n (ossia il numero totale di elementi della permutazione), si ha che:

$$\sum_{j=1}^{k} d_j - 1 = \sum_{j=1}^{k} d_j - \sum_{j=1}^{k} 1 = n - k$$

- Concludiamo quindi che σ' è composto da $n - k$ trasposizioni adiacenti, implicando quindi che:

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

Capitolo 6

Morfismi

Definition 44

Date due strutture algebriche $(G, \cdot)$ e $(H, \cdot)$ dello stesso tipo (dunque entrambi monoidi, gruppi, anelli, ...), definiamo come **morfismo** una funzione $f : G \to H$ tale che:

$$f(gh) = f(g) \cdot f(h), \forall g, h \in G$$

Attenzione:

Nel caso di anelli o strutture algebriche definite su più di una operazione binaria, è necessario **verificare la condizione di morfismo per tutte le operazioni**.

Ad esempio, nel caso in cui $(A, +, \cdot)$ e $(B, +, \cdot)$, la funzione $f : A \to B$ viene detta morfismo se e solo se:

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

Observation 20

Se $(G, \cdot)$ è un gruppo con elemento neutro 1_G, $(H, \cdot)$ è un gruppo con elemento neutro 1_H e $f : G \to H$ è un morfismo, allora:

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

Dimostrazione:

1. Dato $g \in G$, ne segue che:

$$f(g) = f(1_G \cdot g) = f(1_G)f(g) \implies f(g)f(g)^{-1} = f(1_G)f(g)f(g)^{-1} \implies$$

$$\implies 1_H = f(1_G) \cdot 1_H \implies f(1_G) = 1_H$$

2. Dato $g \in G$ e dato $f(1_G) = 1_H$, ne segue che

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

Observation 21

Se $f : G \to H$ è un **morfismo biettivo**, allora $f^{-1} : H \to G$ è un morfismo biettivo. Di conseguenza, $\forall g, h \in H$ si ha che:

$$f^{-1}(gh) = f^{-1}(g)f^{-1}(h)$$

Dimostrazione:

- Supponiamo che f^{-1} sia un morfismo biettivo. Dati $h, h' \in H$, si ha che:

$$f^{-1}(hh') = f^1(h)f^{-1}(h') \implies f(f^{-1}(hh')) = f(f^1(h)f^{-1}(h')) \implies$$
$$\implies hh' = f(f^{-1}(h)) \cdot f(f^{-1}(h')) \implies hh' = hh'$$

Definition 45. Isomorfismo

Date due strutture algebriche G, H e dato il morfismo $f : G \to H$, se f è anche una funzione biettiva essa viene definita come **isomorfismo**

In tal caso, diciamo che G è **isomorfo** ad H (in simboli: $G \cong H$)

Esempi:

1. Definiamo come **radice n-esima dell'unità** (ossia 1) un numero $z \in \mathbb{C}$ 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 $(z_0, ..., z_{n-1})$ 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)

   A questo punto, definiamo

$$H : \{\texttt{radici n-esime di 1 in } \mathbb{C}\} : \{\zeta^0, ..., \zeta^{n-1}\}$$

   Dimostriamo che $(H, \cdot) \subseteq (\mathbb{C}^*, \cdot)$ è sottogruppo:

   - $1 = \zeta^0 \implies 1 \in H$
   - $z, w \in H \iff z^n = w^n = 1 \implies 1 = z^n w^n = (zw)^n \implies zw \in H$

- $z \in H \iff z^n = 1 \implies (z^{-1})^n = (z^n)^{-1} = 1^{-1} = 1 \implies z^{-1} \in H$

Vogliamo verificare che la funzione

$$f : (\mathbb{Z}_n, +) \to (H, \cdot) : [k] \mapsto \zeta^k$$

sia un isomorfismo. Sappiamo già che la funzione è biettiva poiché $|\mathbb{Z}_n| = |H|$. Verifichiamo quindi che sia un morfismo:

$$f([i] + [j]) = f([i])f([j]) \implies f([i + j]) = \zeta^i \cdot \zeta^j \implies f([k]) = \zeta^{i+j} \implies \zeta^k = \zeta^{i+j}$$

A questo punto, è necessario sottolineare che $[i]+[j] = [k] \implies i+j = k+nh, \exists h \in \mathbb{Z}$ (dove n ricordiamo essere la base di $\mathbb{Z}_n$). Di conseguenza, si ha che:

$$\zeta^k = \zeta^{i+j} \implies \zeta^k = \zeta^{k+nh} \implies \zeta^k = \zeta^k \cdot (\zeta^n)^h \implies \zeta^k = \zeta^k \cdot 1^h \implies \zeta^k = \zeta^k$$

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

$$f(n + m) = g^{n+m} = g^n \cdot g^m = f(n)f(m)$$

Come dimostrato nella sezione 4.8, siccome $o(g) < +\infty$, allora $g^n = 1_G = g^0$ per qualche $n > 0$, implicando che $\exists n \neq 0 \mid g^n = g^0$, dunque f non può essere iniettiva.

Vogliamo quindi verificare che tale f possa essere iniettiva se e solo se $o(g) = +\infty$:

- Siccome $o(g) < +\infty \implies f$ `non iniettiva`, allora la negazione di tale affermazione implica che $o(g) = +\infty \implies f$ `iniettiva`
- Supponiamo per assurdo che f non sia iniettiva. Ciò implicherebbe che:

$$\exists n \neq m \mid g^n = g^m \implies g^0 = 1_G = g^{-n} \cdot g^n = g^{-n} \cdot g^m = g^{m-n} \implies$$

$$\implies \exists m - n \neq 0 \mid g^{m-n} = 1_G$$

Come visto nella sezione 4.8, poiché $I(g) = I(d)$ e poiché $d > 0$ (dato che $\exists m - n \neq 0 \mid g^{m-n} = 1_G$, dunque $I(d)$ non può essere l'ideale principale generato da $d = 0$), ne può seguire solo che $o(g) = d$, dunque $o(g) < +\infty$.

Di conseguenza, concludiamo che f `non iniettiva` $\implies o(g) = +\infty$

3. La funzione $f : (\mathbb{Z}, +, \cdot) \to (\mathbb{Z}_n, +, \cdot) : k \mapsto [k]$ è un morfismo di anelli, poiché sia $[a + b] = [a] + [b]$ e $[ab] = [a][b]$ sono entrambi verificati per definizione stessa dell'operazione somma e prodotto su $\mathbb{Z}_n$

4. La funzione $f : (\mathbb{Z}_m, +, \cdot) \to (\mathbb{Z}_\ltimes, +, \cdot) : \texttt{x mod m} \to \texttt{x mod n}$ è un morfismo se e solo se $n \mid m$:

$$\texttt{x mod m} \ + \ \texttt{y mod m} = \texttt{(x+y) mod m} = \texttt{(x+y) mod n}$$

$$\texttt{x mod m} \ \cdot \ \texttt{y mod m} = \texttt{(xy) mod m} = \texttt{(xy) mod n}$$

Attenzione: l'ultimo passaggio di entrambe le equazioni è possibile se e solo se $n \mid m$.

5. Dati i gruppi $(G, \cdot)$ e $(Bij(G), \circ)$, dove $Bij(G)$ è l'insieme di tutte le funzioni biettive di G, allora la funzione $f : G \to Bij(G) : g \mapsto Lg$, dove $Lg : G \to G : h \mapsto gh$, è un morfismo iniettivo $\forall k \in \mathbb{Z}$:

$$(L_g \circ L_h)(k) = L_{gh}(k) \implies L_g(L_h(k)) = (gh)k \implies g(h(k)) \implies ghk = ghk$$

6. Dato il gruppo $(G, \cdot)$ e $g \in G$, la funzione $F_g : G \to G : h \mapsto ghg^{-1}$ è un morfismo:

$$F_g(h)F_g(h') = (ghg^{-1})(gh'g^{-1}) = ghh'g^{-1} = F_g(hh')$$

6.1 Nucleo ed Immagine di un morfismo

Proposition 34. Nucleo ed Immagine di un morfismo

Ogni morfismo $f : G \to H$ tra due gruppi G, H (o altre strutture da essi derivanti, ad esempio anelli) determina un sottogruppo $Ker(f) \subseteq G$, detto **nucleo di** f, e un sottogruppo $Im(f) \subseteq H$, detto **immagine di** f, dove:

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

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

Dimostrazione:

- $Ker(f) \subseteq G$:
  - $f(1_G) = 1_H \implies 1_G \in Ker(f)$
  - $x, y \in Ker(f) \implies f(x) = f(y) = 1_H \implies f(xy) = f(x)f(y) = 1_H \cdot 1_H = 1_H \implies xy \in Ker(f)$
  - $x \in Ker(f) \implies f(x) = 1_H \implies 1_H = 1_H^{-1} = f(x)^{-1} = f(x^{-1}) \implies x^{-1} \in Ker(f)$

- $Im(f) \subseteq H$:
  - $f(1_G) = 1_H \implies 1_G \in Im(f)$
  - $x, y \in Im(f) \implies x = f(g), y = f(h) \implies xy = f(g)f(h) = f(gh) \implies xy \in Im(f)$
  - $x \in Im(f) \implies x = f(g) \implies x^{-1} = f(g)^{-1} = f(g^{-1}) \implies x^{-1} \in Im(f)$

Observation 22

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

Dimostrazione:

- Sappiamo già che $1_G \in Ker(f)$ è sempre valido. Supponendo f iniettiva, si ha che:

$$x \in Ker(f) \implies f(x) = 1_H = f(1_G) \iff x = 1_G$$

- Supponiamo $Ker(f) = \{1_G\}$. In tal caso si ha che:

  $$g, g' \in Ker(f) \implies f(g) = f(g') \implies f(g)^{-1}f(g) = f(g)^{-1}f(g') \implies 1_H = f(g) = f(g^{-1}g')$$

  Siccome 1_G è l'unico elemento appartenente a $Ker(f)$, ne segue che $g^{-1}g' = 1_G \implies g' = g$. Di conseguenza, si ha che

$$g = g' \implies f(g) = f(g')$$

Observation 23

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

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

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

Giustificazione:

Poiché un anello $(A, +, \cdot)$ è un gruppo abeliano nella prima operazione e un monoide nella seconda, ne segue logicamente che il nucleo e l'immagine di f siano determinati dai gruppi $(A, +)$ e $(B, +)$

6.2 Teorema fondamentale di isomorfismo

Definiamo ora una **struttura algebrica intermedia tra sottogruppo ed ideale**, detta sottoanello:

Definition 46. Sottoanello

Dato un anello A definiamo $(B,+,\cdot) \subseteq (A,+,\cdot)$ come sottoanello se:

- $(B,+) \subseteq (A,+)$ è sottogruppo
- $x,y \in B \implies x \cdot y \in B$ (dunque chiusa nella seconda operazione)

Observation 24

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

- $Ker(f)$ è un **ideale** di A
- $Im(f)$ è **sottoanello** di B

Dimostrazione:

- Abbiamo già dimostrato che $(Ker(f),+)$ e $(Im(f),+)$ sono entrambi sottogruppi di A
- $x \in Ker(f), y \in A \implies f(xy) = f(x)f(y) = 0_B \cdot f(y) = 0_B \implies xy \in Ker(f)$
- $x,y \in Im(f) \implies x = f(a), y = f(b), \exists a,b \in A \implies xy = f(a)f(b) = f(ab) \implies xy \in Im(f)$

Theorem 35. Teorema fondamentale di isomorfismo

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

$$A/Ker(f) \cong Im(f)$$

Dimostrazione:

- Mostriamo che esiste $\varphi : A/Ker(f) \to Im(f) : [a] \mapsto f(a)$ e che è **ben definita**, ossia che:
$$[a],[b] \in A/Ker(f) \mid [a] = [b] \implies f(a) = f(b)$$
è vero poichè:
$$[a] = [b] \iff a \equiv b (\mathtt{mod}\ Ker(f)) \iff b - a \in Ker(f) \iff$$
$$\iff 0_B = f(b-a) = f(b) - f(a) \iff f(a) = f(b)$$
- Mostriamo che φ è un **morfismo** sia nel prodotto che nella somma:
$$\varphi([a]) + \varphi([b]) = f(a) + f(b) = f(a+b) = \varphi([a+b])$$
$$\varphi([a])\varphi([b]) = f(a)f(b) = f(ab) = \varphi([ab])$$

- Mostriamo che φ è **iniettiva** poiché il nucleo è semplice:

$$[x] \in A/Ker(f) \mid \varphi([x]) = 0_B \iff f(x) = 0_B \iff x \in Ker(f) \iff [x] = [0_A]$$

- Mostriamo che φ è **suriettiva** per definizione stessa di $Im(f)$

$$b \in Im(f) \iff b = f(a), \exists a \in A \iff b = \varphi([a]), [a] \in A/Ker(f)$$

- Concludiamo quindi che $\varphi : A/Ker(f) \to Im(f)$ è un **isomorfismo**.

Caso particolare in $\mathbb{Z}$

Dato $\zeta := e^{i\frac{2\pi}{n}}$, la funzione seguente funzione è un morfismo:

$$f : (\mathbb{Z}, +, \cdot) \to (\mathbb{C}^*, +, \cdot) : k \mapsto \zeta^k$$

In particolare, si ha che:

$$\zeta^k = 1 \iff n \mid k \implies Ker(f) = I(n)$$

Dimostrazione:

- Vediamo che $I(n) \subseteq Ker(f)$

$$n \mid k \implies k = np \in I(n) \implies \zeta^k = \zeta^{np} = (\zeta^n)^p = 1_H^p = 1_H \in Ker(f)$$

- Vediamo che $Ker(f) \subseteq I(n)$. Per il teorema della divisione col resto euclidea, possiamo esprimere $k \in Ker(f), k = np + r, 0 \leq r < n$

$$1_H = \zeta^k = \zeta^{np+r} = (\zeta^n)^p \cdot \zeta^r = 1_H^p \cdot \zeta^r = \zeta^r$$

  Siccome $\zeta^r = 1_H$ e $0 \leq r < n$, l'unico numero che soddisfa entrambe le condizioni è $r = 0$, dunque:

$$k = np + r = np \in I(n)$$

Inoltre, notiamo inoltre che, per loro definizione stessa, in tal caso si ha che $Im(f) = H(\zeta)$:

$$H(\zeta) : \{\zeta^k \mid k \in \mathbb{Z}\}$$
$$Im(f) : \{z \in \mathbb{C}^* \mid, z = f(k) = \zeta^k, \exists k \in \mathbb{Z}\}$$

Corollary 10

Dato il morfismo $f : (\mathbb{Z}, +, \cdot) \to (\mathbb{C}^*, +, \cdot) : k \mapsto \zeta^k$, per il teorema fondamentale di isomorfismo si ha che:

$$H(\zeta) = Im(f) \cong \mathbb{Z}/Ker(f) = \mathbb{Z}/I(n) = \mathbb{Z}_n$$

6.3 Sottogruppi normali

Abbiamo visto come gli ideali siano un concetto fondamentale all'interno degli anelli. Vediamo ora un concetto egualmente fondamentale all'interno dei gruppi, ossia i **sottogruppi normali**.

Observation 25

Se A è un anello e $B \subseteq A$ un suo sottoanello, $(A/B, +)$ è un gruppo abeliano con la somma $[x] + [y] = [x + y]$.

Se B è solo un sottoanello e non anche un ideale, allora il prodotto $[x][y] = [xy]$ non è ben definito, dunque $(A/B, +, \cdot)$ non è un anello commutativo

Giustificazione:

- Per dimostrare che il prodotto fosse ben definito, viene utilizzata la proprietà di chiusura esterna del prodotto degli ideali (ossia $x \in I, a \in A \implies xa \in I$)

Definiamo quindi un concetto analogo alle classi laterali sinistre, ossia le **classi laterali destre**, le quali ci permetteranno di dimostrare che il prodotto sia ben definito.

Definition 47. Classi laterali sinistre e destre

Sia $(G, \cdot)$ un gruppo e sia $H \subseteq G$ sottogruppo. Possiamo definire due relazioni di equivalenza del tipo:

$$x \sim_S y \iff x^{-1}y \in H \qquad x \sim_D y \iff xy^{-1} \in H$$

Definiamo le classi di equivalenza generate da tali relazioni come **classi laterali sinistre** (per la prima relazione) e **classi laterali destre** (per la seconda relazione).

$$[x]_S : \{y \in G \mid x \sim_S y\} \qquad [x]_D : \{y \in G \mid x \sim_D y\}$$

Observation 26

Come visto nella sezione 4.1.1, si ha che:

$$[x]_S = xH = \{xh \mid h \in H\} \qquad [x]_D = Hx = \{hx \mid h \in H\}$$

Observation 27

La classe dell'elemento neutro di G è sia una classe laterale sinistra sia una classe laterale destra:

$$[1_G]_S = 1_G \cdot H = H = H \cdot 1_G = [1_G]_D$$

Observation 28

Se il sottogruppo non è commutativo, non è detto che $xH = Hx, \forall x \in G$ (si pensi ad esempio alle permutazioni)

Definition 48. Sottogruppo normale

Sia $(G, \cdot)$ un gruppo e sia $H \subseteq G$ sottogruppo. Se si verifica che $xH = Hx$, allora tale sottogruppo viene definito **sottogruppo normale**

Attenzione: ciò non implica che il sottogruppo sia commutativo, ossia che $xh = hx, , \forall x \in G, \forall h \in H$

Proposition 36

Dato $(G, \cdot)$ gruppo e $H \subseteq G$ sottogruppo, le seguenti condizioni sono **equivalenti tra loro**:

1. H è un sottogruppo normale
2. $\forall g \in G, h \in H \implies ghg^{-1} \in H$
3. $g \in G, h \in H \implies \exists k \in H \mid gh = kg$

Dimostrazione:

Le tre condizioni si implicano vicendevolmente, creando una catena (1) $\implies$ 3) $\implies$ 2) $\implies$ 1)) risultante quindi in un se e solo per ognuna di esse:

- 1) $\implies$ 3)
$$gh \in gH = Hg = \{kg \mid k \in H\} \implies gh = kg$$
- 3) $\implies$ 2)
$$g \in G, h \in H \implies \exists k \in H \mid gh = kg \implies ghg^{-1} = kgg^{-1} \implies ghg^{-1} = k \in H$$
- 2) $\implies$ 1)
  - Prendiamo $gh \in gH$ e definiamo $ghg^{-1} =: k \in H$
  - Allora si ha che
  $$ghg^{-1} = k \implies ghg^{-1}g = kg \implies gh = kg \implies kg \in Hg \implies gH \subseteq Hg$$
  - Prendiamo $xg \in Hg$ e definiamo $g^{-1}x(g^{-1})^{-1} = g^{-1}xg =: j \in H$
  - Allora si ha che
  $$g^{-1}xg = j \implies gg^{-1}xh = gj \implies gj \in gH \implies Hg \subseteq gH$$
  - Siccome $gH = Hg$, allora H è normale

Observation 29

La condizione 2) è equivalente a richiedere che H sia l'unione di tutte le classi di equivalenza della relazione di coniugio

Observation 30

Un sottogruppo di un gruppo abeliano è sempre normale, poiché la condizione $xH = Hx$ viene soddisfatta dalla proprietà commutativa

Proposition 37

Se $(G, \cdot)$ è un gruppo e $H \subseteq G$ è un sottogruppo normale, allora $(G/H, \cdot)$ è un gruppo dove il prodotto è ben definito

Dimostrazione:

- Dimostriamo che che $[x][y] = [xy]$ sia ben definito, ossia che $[x] = [x'], [y] = [y'] \implies [xy] = [x'y']$
  - Poiché H è normale, si ha che:

$$xH = Hx = [x] = [x'] = x'H = Hx'$$

$$yH = yx = [y] = [y'] = y'H = Hy'$$

  - Di conseguenza, si verifica che:

$$[x] = [x'] = xH = x'H \implies x' = xh, \exists h \in H$$

$$[y] = [y'] = y'H \implies \exists h \in H, hy' \in Hy = yH \implies \exists k \in H, hy' = yk$$

  - Infine, otteniamo che:

$$x'y' \in (x'y')H \implies x'y' = (xh)y' = xhy' = x(yk) = xyk \in xyH \implies [x'y'] = [xy]$$

- Dimostriamo quindi che $(G/H, \cdot)$ sia un gruppo
  - $([x][y])[z] = [xy][z] = [xyz] = [x][yz] = [x]([y][z])$
  - L'elemento neutro è $[1_G]$
  - L'elemento inverso è $[x^{-1}] = [x]^{-1}$

Corollary 11

Se $f : G \to H$ è un morfismo di gruppi, allora $Ker(f) \subseteq G$ è sottogruppo normale e $Im(f) \subseteq H$ è sottogruppo

Dimostrazione:

- Sappiamo già che $Ker(f) \subseteq G$ e che $Im(f) \subseteq H$ siano entrambi sottogruppi
- Verifichiamo quindi che $Ker(f)$ sia normale utilizzando la condizione 2):

$$g \in G, h \in Ker(f) \implies f(ghg^{-1}) = f(g)f(h)f(g)^{-1}$$

Siccome $h \in Ker(f) \implies f(h) = 1_H$, allora:

$$f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g)f(g)^{-1} = 1_H \implies ghg^{-1} \in Ker(f)$$

A questo punto, possiamo affermare una versione ancora più generica del teorema fondamentale di isomorfismo:

Theorem 38. Teorema fondamentale di isomorfismo

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

$$G/Ker(f) \cong Im(f)$$

Dimostrazione:

- Poiché $Ker(f)$ è un sottogruppo normale, 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 6.2)

Esempio:

- Sia G un gruppo. La funzione $f : \mathbb{Z} \to G : n \to g^n$ è un morfismo.
- Data la struttura di G e di f, si ha che:

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

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

- Poiché in $\mathbb{Z}$ si ha che: $I(g) = I(d), \exists! d \geq 0$ tale che:
  - $d > 0 \implies o(g) = d$
  - $d = 0 \implies o(g) = +\infty$

  si ha che $\mathbb{Z}/Ker(f) = \mathbb{Z}/I(d)$
- Per il teorema fondamentale di isomorfismo, ne segue che:

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

- Concludiamo quindi che:

$$H(g) \cong \begin{cases} \mathbb{Z} & \text{se } o(g) = +\infty \\ \mathbb{Z}_d & \text{se } o(g) = d \end{cases}$$

Corollary 12

Se G è un gruppo finito dove $|G| = p$ dove $p \in \mathbb{P}$, allora

$$G \cong \mathbb{Z}_p$$

Dimostrazione:

- Poiché $|G| = p$ ne segue che $|H(g)| > 1$.
- Per il teorema di Lagrange, si ha che

$$|H(g)| \mid |G| = p \implies |H(g)| = \begin{cases} 1 \\ p \end{cases}$$

- Poiché abbiamo assunto $|H(g)| > 1$, l'unico caso possibile è che $|H(g)| = p$
- Siccome $|G| = p = |H(g)|$, allora il sottogruppo $H(g)$ coincide esattamente con G
- Seguendo la dimostrazione dell'esercizio precedente, possiamo concludere che

$$G = H \cong \mathbb{Z}_p$$

Corollary 13

Più in generale, se G è un gruppo finito dove $|G| = n, n \in \mathbb{N}$ e $\exists g \in G \mid o(g) = n$, allora:

$$G \cong \mathbb{Z}_n$$

Dimostrazione:

- Supponiamo che $\exists g \in G \mid o(g) = n$. In tal caso, si ha che:

$$o(g) = n \iff H(g) : \{1, g, ..., g^{n-1}\}$$

- Siccome $H(g) \subseteq G$ e $|H|\,(g) = |G|$, allora $G = H(g)$
- Infine, siccome $o(g) = n \implies H(g) \cong \mathbb{Z}_n$, allora:

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

Observation 31

Se $H \subseteq G$ è un sottogruppo normale, allora $f : G \to G/H : x \to [x]$ è un morfismo e $Ker(f) = H$

Dimostrazione:

- Verifichiamo che sia un morfismo:

$$f(xy) = [xy] = [x][y] = f(x)f(y)$$

- $Ker(f) = H$:

$$g \in Ker(f) \iff f(g) = [g] = [1_G] = 1_g \cdot H = H \iff g \in H$$

Esempi:

- Dato il gruppo simmetrico S_n, il gruppo alterno $A_n \subseteq S_n$ è un sottogruppo normale

$$\sigma \in A_n, \tau \in S_n \implies \tau\sigma\tau^{-1} \implies sgn(\tau\sigma\tau^{-1}) =$$
$$= sgn(\tau)sgn(\sigma)sgn(\tau^{-1}) = (\pm 1)(+1)(\pm 1) = +1 \implies \tau\sigma\tau^{-1} \in A_n$$

- Dato $X : \{+1, -1\}$, si ha che $X \cong \mathbb{Z}_2$
- La funzione $sgn : S_n \to \{+1, -1\}$ è un morfismo

$$sgn(\sigma\sigma') = sgn(\sigma)sgn(\sigma')$$

  dove si ha che $Ker(f) = A_n$, implicando che $Ker(f)$ sia normale

6.4 Gruppi diedrali

Definition 49. 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)

$$\rho : \texttt{ rotazione antioraria di } \frac{2\pi}{n}$$

- Riflessioni a specchio rispetto agli assi di simmetria del poligono (ogni poligono regolare possiede n assi di simmetria)

$$\sigma_i : \texttt{ riflessione rispetto all'asse di simmetria } r_i$$

Attenzione: il prodotto è dato dalla composizione (dunque viene trattato come nel caso delle permutazioni), ossia $\rho\sigma(i) = \rho(\sigma(i))$

Observation 32

Dato $\mathcal{D}_n$, effettuare n volte una rotazione riporta il poligono allo stato iniziale (poiché $n \cdot \frac{2\pi}{n} = 2\pi$), dunque

$$\rho^n = \rho^0 = 1 \implies \rho^{n+k} = \rho^n \rho^k = \rho^0 \rho^k = \rho^k$$

Analogamente, poiché un poligono regolare di n lati possiede solo n assi di simmetria, si ha che:

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

Observation 33

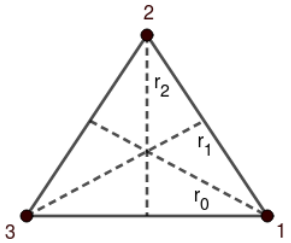
Per definizione stessa, ogni riflessione a specchio è uguale alla sua inversa.

Dunque, riflettere due volte rispetto allo stesso asse corrisponde alla simmetria neutra, ossia $\rho^0 = 1$

$$\sigma_i = \sigma_i^{-1} \implies \sigma_i^2 = 1$$

Esempi:

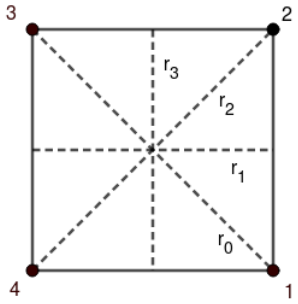
- Consideriamo il gruppo $\mathcal{D}_3$, corrispondente alle simmetrie di un triangolo equilatero.



  In tal caso, abbiamo che:

$$\mathcal{D}_3 : \{1, \rho, \rho^2, \sigma_0, \sigma_1, \sigma_2\}$$

- Consideriamo il gruppo $\mathcal{D}_4$, corrispondente alle simmetrie di un quadrato.

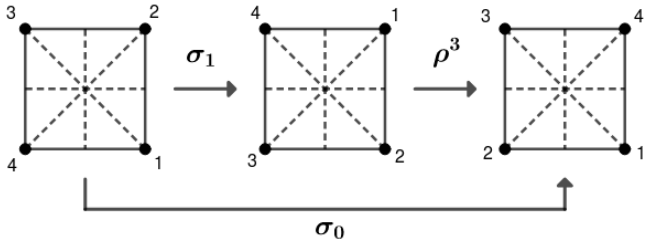


  In tal caso, abbiamo che:

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

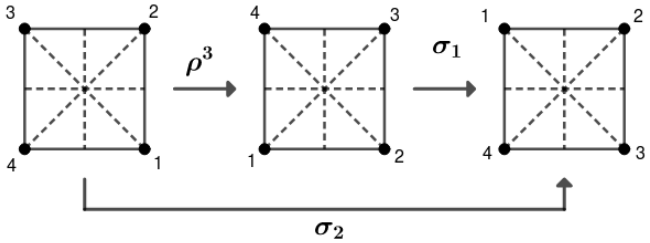
Notiamo inoltre come in $\mathcal{D}_4$ si ha:

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



E che:

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



Dunque, concludiamo che il prodotto non sia commutativo:

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

Observation 34

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

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

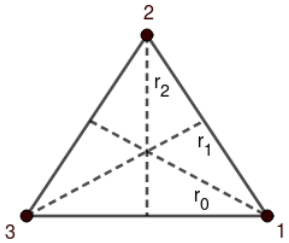
Proposition 39

Numerando i vertici del poligono, ogni simmetria **corrisponde** ad una permutazione dei vertici, dunque si verifica che $\mathcal{D}_n$ è **iniettivamente incluso** in $\mathcal{S}_n$.

In generale, se $\alpha \in \mathcal{D}_n$, ovvero una simmetria del poligono regolare di n lati, manda il vertice i nel vertice j, allora la corrispondente permutazione $\sigma_\alpha \in \mathcal{S}_n$ manderà anch'essa i in j

Esempio:

- Consideriamo il gruppo $\mathcal{D}_3$, numerando i vertici del triangolo corrispondente



  In tal caso abbiamo che:

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

Corollary 14

Dato il gruppo $\mathcal{D}_n$ e il sottogruppo $H \subseteq \mathcal{S}_n$ dove:

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

Si ha che:

$$\mathcal{D}_n \cong H \subseteq \mathcal{S}_n$$

Dimostrazione:

- Siccome ad ogni simmetria in $\mathcal{D}_n$ corrisponde una permutazione in $H \subseteq \mathcal{S}_n$, allora:

$$\begin{cases} \alpha, \sigma_\alpha : i \mapsto j \\ \beta, \sigma_\beta : j \mapsto k \end{cases} \implies \beta\alpha, \sigma_\beta\sigma_\alpha : i \mapsto k$$

  dunque si ha che $\sigma_{\beta\alpha} = \sigma_\beta\sigma_\alpha$

- Dati i vertici del poligono $v_1, \ldots, v_n$ si quindi verifica che:

$$\alpha(v_i) = v_{\sigma_\alpha(i)}$$

- La funzione $f : (\mathcal{D}_n, \cdot) \to (H \subseteq \mathcal{S}_n, \cdot) : \alpha \mapsto \sigma_\alpha$ è un morfismo (ricordiamo che in entrambi i gruppi il prodotto è dato dalla composizione)

$$\alpha\beta(v_i) = \alpha(\beta(v_i)) = \alpha(v_{\sigma_\beta(i)}) = v_{\sigma_\alpha(i)\sigma_\beta(i)} = v_{\sigma_{\alpha\beta}(i)}$$

- In particolare, f è un isomorfismo poiché ad ogni simmetria corrisponde una ed una sola permutazione, implicando quindi che f sia iniettiva

6.5 Gruppo di Klein e Teorema di Cauchy

Definition 50. Gruppo di Klein

Definiamo come **gruppo di Klein** (o gruppo quadrinomio) il più piccolo gruppo non ciclico:

$$\mathcal{K}_4 : \{1, a, b, c\}$$

dove si verifica che:

- $a^2 = b^2 = c^2 = 1 \implies o(a) = o(b) = o(c) = 2$
- $ab = ba = c$
- $bc = cb = a$
- $ac = ca = b$

Esempio:

- Consideriamo il gruppo $\mathcal{D}_2 : \{1, \rho, \sigma_0, \sigma_1\}$. Notiamo come:
  - $\rho^2 = \sigma_0^2 = \sigma_1^2 = 1$
  - $\rho\sigma_0 = \sigma_0\rho = \sigma_1$
  - $\rho\sigma_1 = \sigma_1\rho = \sigma_0$
  - $\sigma_1\sigma_0 = \sigma_0\sigma_1 = \rho$

  Dunque, concludiamo facilmente che $\mathcal{D}_2 \cong \mathcal{K}_4$

Proposition 40

Sia G un gruppo finito dove $|G| = 4$. Allora, 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 $o(a) \mid |G| = 4 \iff o(g) = 1, 2, 4$
- Come visto nella sezione 6.3, sappiamo che

$$\exists a \in G \mid o(a) = 4 \implies G \cong \mathbb{Z}_4$$

- Ipotizziamo ora che non sia ciclico. Se invece $G : \{1, a, b, c\}$ 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 $ab \neq c$, allora l'unica possibilità affinché valga la chiusura del gruppo è $ab = c$

- Analogamente, dimostriamo che $ac = b$ e $bc = a$, concludendo quindi che:

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

Theorem 41. Teorema di Cauchy

Dato un gruppo finito G e un numero primo $p \in \mathbb{P}$, si verifica che:

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

In particolare, se $|G| = q \in \mathbb{P}$, allora G è ciclico poiché

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

Proposition 42

Sia G un gruppo finito dove $|G| = 6$. Allora, 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 ora che non sia ciclico. Per il teorema di Cauchy sappiamo che
  - $\exists \alpha \in G \mid o(\alpha) = 3 \implies o(\alpha^k) = 3, k \neq 0$
  - $\exists \beta \in G \mid o(\beta) = 2 \implies \beta^{-1} = \beta$
- 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:

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

  di conseguenza si ha che $\beta \neq \alpha^{i-j}$.

- Mostriamo inoltre che $\beta\alpha = \alpha^2\beta$:
  - Supponiamo per assurdo che $\beta\alpha = 1$

$$\beta\alpha = 1 \implies \alpha = \beta^{-1} \implies \alpha = \beta$$

    il che è impossibile
  - Supponiamo per assurdo che $\beta\alpha = \alpha$

$$\beta\alpha = \alpha \implies \beta = 1$$

    il che è impossibile
  - Supponiamo per assurdo che $\beta\alpha = \alpha^2$

$$\beta\alpha = \alpha^2 \implies \beta = \alpha$$

    il che è impossibile
  - Supponiamo per assurdo che $\beta\alpha = \beta$

$$\beta\alpha = \beta \implies \alpha = 1$$

    il che è impossibile
  - Supponiamo per assurdo che $\beta\alpha = \alpha\beta$, implicando che $o(\beta\alpha) = o(\alpha\beta)$:
    - $(\alpha\beta)^1 = \alpha\beta$
    - $(\alpha\beta)^2 = (\beta\alpha)(\beta\alpha) = \beta\beta\alpha\alpha = \beta^2\alpha^2 = \alpha^2$
    - $(\alpha\beta)^3 = (\alpha\beta)(\alpha\beta)^2 = (\alpha\beta)\alpha^2 = \alpha^3\beta = \beta$
    - $(\alpha\beta)^4 = (\alpha\beta)(\alpha\beta)^3 = (\alpha\beta)\beta = \alpha\beta^2 = \alpha$
    - $(\alpha\beta)^5 = (\alpha\beta)(\alpha\beta)^4 = (\alpha\beta)\alpha = \alpha^2\beta$
    - $(\alpha\beta)^6 = (\alpha\beta)(\alpha\beta)^5 = (\alpha\beta)\alpha^2\beta = \beta^2\alpha^3 = 1$

    dunque $o(\alpha\beta) = 6 \implies o(\alpha\beta) = |G| \implies G = H(\beta\alpha)$, ossia che il gruppo sia ciclico, contro l'ipotesi che invece esso non lo sia.
  - Quindi l'unica possibilità è che $\beta\alpha = \alpha^2\beta$

- Concludiamo quindi che:

$$G = \{1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$$

- A questo punto, possiamo stendere una **tavola di Cayley**, ossia una tavola moltiplicativa:

	1	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
1	1	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
α	α	α^2	1	$\alpha\beta$	$\alpha^2\beta$	β
α^2	α^2	1	α	$\alpha^2\beta$	β	$\alpha\beta$
β	β	$\alpha^2\beta$	$\alpha\beta$	1	α^2	α
$\alpha\beta$	$\alpha\beta$	β	$\alpha^2\beta$	α	1	α^2
$\alpha^2\beta$	$\alpha^2\beta$	$\alpha\beta$	β	α^2	α	1

- A questo punto, ricordando le proprietà dei prodotti dei gruppi diedrali (sezione 6.4), 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 $\mathcal{D}_3 \cong H \subseteq \mathcal{S}_3$ dove

$$H : \{\sigma_\alpha \in \mathcal{S}_3 \mid \sigma_\alpha = \alpha, \alpha \in \mathcal{D}_3\}$$

  e dove $|\mathcal{D}_3| = 2 \cdot 3 = 6$ e $|\mathcal{S}_n| = 3! = 6$.

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

  Tuttavia, si ha che $H \subseteq \mathbb{S}_3 \wedge |H| = |\mathcal{S}_3| \implies H = \mathbb{S}_3$, dunque concludiamo che:

$$G \cong \mathcal{D}_3 \cong H = \mathcal{S}_3$$

Capitolo 7

Polinomi

Definition 51. Anello polinomiale

Dato un anello commutativo A definiamo l'**insieme dei polinomi** aventi come coefficienti elementi in A come:

$$A[x] : \{a_0 + a_1x + \ldots + a_nx^n \mid a_0, \ldots, a_n \in A, a_n \neq 0\}$$

Inoltre, $A[x]$ risulta essere un **anello commutativo**

Dimostrazione:

- Dati due polinomi $p(x), q(x) \in A[x]$, dunque definiti come

$$p(x) = \sum_{i=0}^{n} a_i x^i \qquad q(x) = \sum_{i=0}^{m} b_i x^i$$

  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:

$$\forall p(x) \in A[x], \exists -p(x) \in A[x] \mid p(x) + (-p(x)) = 0$$

- L'elemento inverso nel prodotto non esiste poiché, per via della definizione data di polinomio, non esiste un inverso moltiplicativo.

  Si pensi ad esempio a $p(x) = x$. Tale polinomio non ammette inverso moltiplicativo poiché $\frac{1}{x}$ non è un polinomio.

  Di conseguenza, $A[x]$ non può essere un campo.

Proposition 43

Ogni elemento $a \in A$ può essere visto come un polinomio costante $p(x) = a \in A[x]$. Dunque, si ha che $A \subseteq A[x]$

Observation 35

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

Definition 52. 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)
- $p(x) = a_0 + a_1x + \ldots + a_nx^n \neq 0, a_n \neq 0 \iff deg(p(x)) = n$

Definition 53. Coefficienti direttori

Dato $p(x) = a_0+a_1x+\ldots+a_nx^n \neq 0 \in A[x]$ definiamo a_n come **coefficiente direttore** del polinomio

Observation 36

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

$$p(x) \cdot q(x) = \sum_{i=0}^{n} \left(\sum_{j=0}^{m} a_i b_j x^{i+j} \right) = a_0b_0 + a_0b_1x^1 + \ldots + a_nb_mx^{n+m}$$

  allora $deg(p(x)q(x)) = deg(p(x)) + deg(q(x)) = n + m$

Proposition 44

Gli unici elementi invertibili di $K[x]$ sono i polinomi costanti, dunque

$$K[x]^* = K^* \subseteq K \subseteq K[x]$$

Dimostrazione:

- Siccome $\forall a(x), b(x) \in K[x]$ si ha che

  $$deg(a(x)b(x)) \geq deg(a(x)) \geq 1$$

  e dato che $deg(1) = 0$, allora

  $$\nexists a(x)^{-1} \in K[x] \mid deg(a(x)a(x)^{-1}) = deg(1) \geq 1$$

  Dunque

  $$def(a(x)) \geq 1 \implies a(x)^{-1} \notin K[x]^*$$

- Tale dimostrazione, inoltre, riprova che non esista sempre un invertibile moltiplicativo in $K[x]$
- Se invece $deg(a(x)) = 0$, allora $\exists a_0 \neq 0 \in K \mid a(x) = a_0 \implies a(x) \in K$.
- Poiché K è un campo, ogni elemento è invertibile, dunque $\exists a_0^{-1} \in K$
- Posto quindi $b_0 := a_0^{-1}$ e $b(x) = b_0$, allora

  $$a(x)b(x) = a_0 b_0 = a_0 a_0^{-1} = 1$$

- Dunque, ogni polinomio costante è invertibile, implicando che, poiché ogni polinomio costante appartiene anche a K, allora

  $$K[x]^* = K^* \subseteq K \subseteq K[x]$$

7.1 Divisione con resto di polinomi

Theorem 45. 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 $deg(r_1(x)), deg(r_2(x)) < deg(b(x))$

- Quindi deduciamo 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:

$$b(x)q_1(x) + r_1(x) = b(x)q_2(x) + r_2(x) \implies b(x)[q_1(x) - q_2(x)] = r_2(x) - r_1(x) \implies$$

$$\implies deg(r_2(x) - r_1(x)) = deg(b(x)) + deg(q_1(x) - q_2(x))$$

- Se $deg(q_1(x) - q_2(x)) \geq 0$ avremmo $deg(r_2(x) - r_1(x)) \geq deg(b(x))$, contraddicendo l'ipotesi
- Di conseguenza, l'unica possibilità è:

$$q_1(x) - q_2(x) = 0 = r_1(x) - r_2(x)$$

e dunque che $q_1(x) = q_2(x)$ e $r_1(x) = r_2(x)$

Esempio:

- Calcolo della divisione con resto di $a(x) = 2x^4 + 3x^3 - 2x^2 + x - 4$ e $b(x) = x^2 - x + 1$

$+2x^4$	$+3x^3$	$-2x^2$	$+x$	-4	$+x^2$	$-x$	$+1$
$-2x^4$	$+2x^3$	$-2x^2$			$2x^2$	$+5x$	$+1$
	$+5x^3$	$-4x^2$	$+x$	-4			
	$-5x^3$	$+5x^2$	$-5x$				
		x^2	$-4x$	-4			
		$-x^2$	$+x$	-1			
			$+3x$	-5			

Quindi concludiamo che:

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

7.1.1 Regola di Ruffini

Method 3. 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 $a(x) = a_0 + \ldots + a_n x^n$ 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
$$q(x) = q_0 + \ldots + q_{n-1}x^{n-1}$$
dove $q_0, \ldots, q_{n-1}$ 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}	$\ldots$	a_1	a_0
c		cq_{n-1}	$\ldots$	cq_1	cq_0
	q_{n-1}	q_{n-2}	$\ldots$	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:
$$x^4 - 3x^3 + 2x - 5 = (x + 2)(x^3 - 5x^2 + 10x - 18) + 31$$

Proposition 46. Teorema del fattore

Dato $p(x) \in K[x]$ e dato $c \in K$
$$p(c) = 0 \iff x - c \mid p(x)$$
in tal caso, c viene detta **radice (o zero) del polinomio**

Dimostrazione:

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

- $p(c) = 0 \implies x - c \mid p(x)$
  - Siano $q(x)$ e $r(x)$ il quoziente e il resto della divisione di $p(x)$ per $(x - c)$

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

  - Per ipotesi, si ha che:

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

    dunque, la divisione non ha resto, implicando che:

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

Corollary 15

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 $c_1, \ldots, c_m$ 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:

$$\begin{cases} x - c_1 \mid p(x) \\ \vdots \\ x - c_m \mid p(x) \end{cases} \implies \underbrace{(x - c_1) \cdot \ldots \cdot (x - c_m)}_{q(x)} \mid p(x)$$

- 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

Observation 37

L'anello commutativo $K[x]$ è un **dominio di integrità** poiché

$$\nexists p(x) \neq 0 \in K[x] \mid p(x) \mid 0$$

Corollary 16

Poiché $K[x]$ è un dominio di integrità, dati $p(x), q(x) \in K[x]$ si ha che:

$$I(p(x)) = I(q(x)) \iff p(x) = c \cdot q(x), \exists c \in K[x]^*$$

(dimostrazione nella sezione 4.3)

Theorem 47

L'anello commutativo $K[x]$ è un **dominio ad ideali principali**, dunque

$$\exists! p(x) \in K[x] \mid I = I(p(x)$$

Dimostrazione unicità:

- Se $I = \{0\}$, allora $I = I(0)$
- Sia invece $p(x) \neq 0 \in I$ il polinomio del più piccolo grado possibile all'interno dell'ideale tale che $I = I(p(x))$. Ciò implica che

$$q(x) \in K[x] \mid deg(q(x)) < deg(p(x)) \implies q(x) = 0$$

Dimostrazione esistenza:

- $I \subseteq I(p(x))$
  - Sia $p(x) \neq 0 \in I$ il polinomio del grado più piccolo possibile all'interno dell'ideale.
  - Dato $a \in I \mid a(x) = p(x)q(x) + r(x)$ si ha che $deg(r(x)) < deg(p(x))$. Tuttavia, si ha anche che

    $$a(x), p(x), q(x) \in I \implies r(x) = a(x) - p(x)q(x) \in I$$

    implicando che $r(x)$ sia il polinomio del grado più piccolo possibile (poiché $deg(r(x)) < deg(p(x))$).
  - Ne segue quindi necessariamente che $r(x) = 0 \implies deg(r(x)) = -\infty < deg(p(x))$, dunque che:

    $$r(x) = 0 = a(x) - p(x)q(x) \implies a(x) = p(x)q(x) \in I(p(x))$$

- $I(p(x)) \subseteq I$
  - Dato $p(x)) \neq 0 \in I$ il polinomio del grado più piccolo possibile all'interno dell'ideale, si verifica automaticamente che

    $$p(x) \neq 0 \in I \implies \forall a(x) \in I(p(x)) \mid a(x) = p(x)q(x) \in I$$

    poiché, come già provato nell'implicazione precedente, si ha $r(x) = 0$

Definition 54. MCD di due polinomi

Dati $a(x), b(x) \in K[x]$, definiamo $d(x) := MCD(a(x), b(x))$ il polinomio per cui

$$d(x) \in K[x] \mid I(d(x)) = I(a(x), b(x))$$

dove $I(a(x), b(x)) : \{a(x)p(x) + b(x)q(x), \exists p(x), q(x) \in K[x]\}$

In particolare, individuiamo l'analogo dell'**identità di Bezout**:

$$\exists p(x), q(x) \mid a(x)p(x) + b(x)q(x) = d(x)$$

Definition 55. mcm di due polinomi

Dati $a(x), b(x) \in K[x]$, definiamo $m(x) := mcm(a(x), b(x))$ il polinomio per cui

$$m(x) \in K[x] \mid I(m(x)) = I(a(x)) \cap I(b(x))$$

Corollary 17

Dalle due definizioni date, ne segue naturalmente che:

$$p(x) \mid a(x) \wedge p(x) \mid b(x) \implies p(x) \mid d(x) := MCD(a(x), b(x))$$

e che:

$$a(x) \mid q(x) \wedge b(x) \mid q(x) \implies m(x) := mcm(a(x), b(x)) \mid q(x)$$

Observation 38

Poiché $K[x]$ è un dominio dominio di integrità, sappiamo che

$$I(p(x)) = I(q(x)) \iff p(x) = c \cdot q(x), \exists c \in K[x]^*$$

Ciò implica che dati $a(x), b(x) \in K[x]$, si ha che $d(x) := MCD(a(x), b(x))$ e $m(x) := mcm(a(x), b(x))$ possano essere ben definiti solo a meno di una costante moltiplicativa non nulla.

Affinché valga l'unicità, basta imporre che i polinomi $d(x)$ e $m(x)$ abbiano coefficiente direttore $a_n = 1$

Definition 56. Polinomio monico

Dato $a(x) = a_0 + \ldots + a_n x^n \in K[x]$, definiamo $a(x)$ come **polinomio monico** se $a_n = 1$

Method 4

Dati $a(x), b(x) \in K[x]$, possiamo calcolare $d(x) := MCD(a(x), b(x))$ tramite l' **algoritmo di Euclide** e $m(x) := mcm(a(x), b(x))$ tramite il **teorema fondamentale dell'aritmetica**:

$$m(x) = \frac{a(x)b(x)}{d(x)}$$

Observation 39

Dati polinomi $a(x), b(x) \in K[x], c \in K$ e sia $d(x) := MCD(a(x), b(x)) \in K[x]$. Allora si ha che:

$$a(c) = 0 = b(c) \iff d(c) = 0$$

Ovvero le uniche radici in comune tra due polinomi sono le radici del loro MCD

Proposition 48

Dato $p(x) \in K[x]$, esso è irriducibile se e solo se è primo

Dimostrazione:

- Sappiamo già che in un dominio di integrità si ha:

  $$p(x) \texttt{ primo} \implies p(x) \texttt{ irriducibile}$$

  (dimostrazione nella sezione 4.3.1)

- Supponiamo quindi che $p(x) \in K[x]$ sia irriducibile. Dunque si ha che:

  $$d(x) \mid p(x) \implies p(x) = d(x)q(x) \implies d(x) \in K[x]^* \vee q(x) \in K[x]^*$$

- Poiché $K[x]^* = K^*$ allora si verifica che

  $$d(x) \in K[x]^* = K^* \implies d(x) = c \in K^*$$

  oppure che

  $$q(x) \in K[x]^* = K^* \implies q(x) = k \in K^* \implies d(x) = k^{-1}p(x)$$

- Dato $a(x) \in K[x]$, supponiamo che $p(x) \mid a(x)b(x)$ Si ha quindi che:

  $$a(x)b(x) = p(x)q(x), \exists q(x) \in K[x]$$

- Supponiamo che $p(x) \nmid a(x)$. Si ha quindi che $MCD(p(x), a(x)) = 1$.

  Per l'identità di Bezout, si ha che:

  $$\exists f(x), g(x) \in K[x] \mid MCD(p(x), a(x)) = 1 = p(x)f(x) + a(x)g(x) \implies$$
  $$b(x) = p(x)b(x)f(x) + a(x)b(x)g(x) \implies b(x) = p(x)b(x)f(x) + p(x)q(x)g(x) \implies$$
  $$\implies b(x) = p(x)[q(x)f(x) + g(x)b(x)] \implies p(x) \mid b(x) \implies p(x) \mid a(x)b(x)$$

- Se invece $p(x) \mid a(x)$ allora $MCD(p(x), a(x)) \neq 1$, allora $p(x) \nmid b(x)$
- Concludiamo quindi che $p(x) \mid a(x)b(x) \implies p(x) \mid a(x) \vee p(x) \mid b(x)$

Theorem 49. Fattorizzazione in polinomi irriducibili e monici

Dato $p(x) \neq 0 \in K[x]$ allora $\exists! q_1(x), \ldots, q_k(x) \in K[x]$ polinomi irriducibili e monici e $\exists! c \in K^*$ tali che:

$$p(x) = c \cdot q_1(x) \cdot \ldots \cdot q_k(x)$$

Dimostrazione esistenza:

- Se $deg(p(x)) = 1$, allora $p(x)$ è irriducibile (e di conseguenza anche primo).

  Difatti, se esistesse una fattorizzazione di $p(x)$ (dunque non fosse irriducibile) avremmo che:

  $$deg(p(x)) = deg(q_1(x)) + \ldots + deg(q_k(x))$$

  dove $deg(q_i(x)) > 0$ (poiché altrimenti sarebbe una costante), implicando quindi che $deg(p(x)) > 1$ contro l'ipotesi

- Sia quindi $deg(p(x)) > 1$, implicando che $p(x)$ non sia irriducibile, dunque $p(x) = a(x)b(x)$

- Supponiamo per ipotesi induttiva che $a(x)$ e $b(x)$ siano fattorizzati in polinomi irriducibile e monici

  $$a(x) = c \cdot q_1(x) \cdot \ldots \cdot q_k(x)$$
  $$b(x) = c' \cdot q'_1(x) \cdot \ldots \cdot q'_j(x)$$

  si ha quindi che:

  $$p(x) = c \cdot c' \cdot q_1(x) \cdot q'_1(x) \cdot \ldots \cdot \ldots \cdot q_k(x) \cdot q'_j(x)$$

Dimostrazione unicità:

- Se $deg(p(x)) = 0$ allora $p(x) = c$
- Se $deg(p(x)) > 0$, supponiamo due fattorizzazioni possibili per $p(x)$

  $$c \cdot q_1(x) \cdot \ldots \cdot \ldots \cdot q_k(x) = p(x) = c' \cdot q'_1(x) \cdot \ldots \cdot q'_j(x)$$

- Notiamo che se $p(x) = a_0 + a_1 x + \ldots + a_n x^n$, allora $c = a_n = c'$. Supponendo che $q_1(x), \ldots, q_k(x), q'_1(x), \ldots q'_j(x) \in K[x]$ siano monici, allora anche il loro prodotto è monico

  $$p(x) = a_0 + \ldots + a_n x^n = c) = c \cdot q_1(x) \cdot \ldots \cdot q_k(x) = c' \cdot q'_1(x) \cdot \ldots \cdot q'_j(x) \implies$$
  $$\implies q_1(x) \mid p(x) = c' \cdot q'_1(x) \cdot \ldots \cdot q'_j(x) \implies$$
  $$q_1(x) \mid q'_1(x) \vee \ldots \vee q_1(x) \mid q'_j(x)$$

- Supponiamo che $q_1(x) \mid q'_1(x) \implies q'_1(x) = k \cdot q'_1(x), \exists k \in K^*$, implicando che:

  $$c \cdot q_1(x) \cdot \ldots \cdot \ldots \cdot q_k(x) = p(x) = c' \cdot q'_1(x) \cdot \ldots \cdot q'_j(x) \implies$$
  $$\implies c \cdot q_1(x) \cdot \ldots \cdot \ldots \cdot q_k(x) = p(x) = c' \cdot k \cdot q_1(x) \cdot \ldots \cdot q'_j(x) \implies$$
  $$\implies c \cdot q_2(x) \cdot \ldots \cdot \ldots \cdot q_k(x) = \frac{p(x)}{q_1(x)} = c' \cdot k \cdot q'_2(x) \cdot \ldots \cdot q'_j(x)$$

- Poiché $deg(\frac{p(x)}{q(x)}) < deg(p(x))$ possiamo concludere che $k = j$ e, a meno di riordinare i fattori, possiamo assumere che $q_2(x) = q_2'(x), \dots, q_k(x) = q_j'(x)$

Proposition 50

Dato $p(x) \in \mathbb{C}[x]$, esso è irriducibile se e solo se $deg(p(x)) = 1$

Dimostrazione:

- Dato $p(x) \neq 0 \in K[x]$, se $deg(p(x)) > 1$ allora $p(x)$ non è irriducibile poiché per via del teorema fondamentale dell'algebra si ha che:

$$\exists z \in \mathbb{C} \mid p(z) = 0 \iff x - z \mid p(x) \iff$$

$$\iff p(x) = (x - z)q(x), \exists q(x) \in K[x] \implies deg(q(x)) = deg(p(x)) - 1$$

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

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

  e dunque $p(x)$ è irriducibile

Proposition 51

Dato $p(x) \in \mathbb{R}[x]$, esso è irriducibile se e solo se $deg(p(x))$ oppure $p(x) = ax^2 + bx + c \mid \Delta := b^2 - 4ac < 0$

Dimostrazione:

- Se $deg(p(x)) = 1$, la dimostrazione è analoga a quella della proposizione precedente
- Se invece $deg(p(x)) = 2$ e $p(x)$ non ha radici $x_1, x_2 \in \mathbb{R}$, allora $p(x)$ è irriducibile
- Difatti, se $p(x)$ fosse riducibile si avrebbe che:

$$deg(p(x)) = 2 \wedge p(x) = a(x)b(x) \implies \begin{cases} deg(a(x)) = 1 \\ deg(b(x)) = 1 \end{cases}$$

- Se $a(x) = cx + d$ dove $c \neq 0, d \in \mathbb{R}$, allora $x = -c^{-1}d$ sarebbe una radice di $a(x)$ e di conseguenza anche di $p(x)$, contraddicendo l'ipotesi
- Sia quindi $p(x) \in \mathbb{R}[x]$ irriducibile con $deg(p(x)) > 1$. Per il teorema fondamentale dell'algebra, $\exists z \in \mathbb{C} \mid p(z) = 0$. Se tale z fosse anche reale ($z \in \mathbb{R}$), allora si avrebbe che

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

- Dato quindi $p(x) = a_0 + \dots a_n x^n$ dove $a_1, \dots, a_n \in \mathbb{R}$, allora si ha che ogni coefficiente è uguale al suo coniugato (poiché $a_i := c + i \cdot 0 = c - i \cdot 0 =: \overline{a_i}$):

$$a_1, \dots, a_n \in \mathbb{R} \implies a_1 = \overline{a_1}, \dots, a_n = \overline{a_n}$$

- Per le proprietà dei coniugati (sezione 2), si ha che:

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

- Siccome però per ipotesi $p(z) = 0$, allora si ha che anche $\overline{p(z)} = \overline{0} = 0$. Di conseguenza, si ha che anche $\overline{z}$ è una radice di $p(x)$, da cui deriva che:

$$x - z \mid p(x) \wedge x - \overline{z} \mid p(x) \implies (x - z)(x - \overline{z}) \mid p(x) \implies x^2 - (z + \overline{z})x + z \cdot \overline{z} \mid p(x)$$

- Siccome $z + \overline{z} = (c + id)(c - id) = 2c \in \mathbb{R}$ e $z \cdot \overline{z} = (c + id)(c - id) = c^2 + d^2 \in \mathbb{R}$, allora ne segue che $x^2 - (z + \overline{z})x + z \cdot \overline{z} = x^2 - 2c + c^2 + d^2 \in \mathbb{R}$
- Poiché $p(x)$ è irriducibile, in definitiva abbiamo che:

$$p(x) = k(x^2 - 2c + c^2 + d^2), \exists k \in R^*$$

- Possiamo concludere, quindi, che $p(x)$ dove $deg(p(x)) > 1$ è irriducibile se e solo se:

$$\Delta := (-2kc)^2 - 4k^2(c^2 + d^2) = 4k^2c^2 - 4k^2(c^2 + d^2) = -4kd^2 < 0$$

Theorem 52

Sia $p(x) \in \mathbb{Z}[x]$ dove $p(x) = a_0 + \ldots a_n x^n$ con $a_0, a_n \neq 0$. Se $\frac{a}{b} \in \mathbb{Q}$ è radice di $p(x)$ e $MCD(a, b) = 1$, allora

$$p\left(\frac{a}{b}\right) = 0 \implies a \mid a_0 \wedge b \mid a_n$$

Dimostrazione:

- Sia $p(x) = a_0 + \ldots a_n x^n \in \mathbb{Z}[x]$. Supponendo che $\frac{a}{b} \in \mathbb{Q} \mid MCD(a, b) = 1$ sia radice di $p(x)$, allora

$$0 = p\left(\frac{a}{b}\right) = a_0 + a_1 \cdot \left(\frac{a}{b}\right) + \ldots + a_n \cdot \left(\frac{a}{b}\right)^n \implies$$
$$\implies b^n \cdot 0 = b^n \left(a_0 + a_1 \cdot \left(\frac{a}{b}\right) + \ldots + a_n \cdot \left(\frac{a}{b}\right)^n\right) \implies$$
$$\implies 0 = a_0 b^n + \ldots + a_{n-1} \cdot a^{n-1} \cdot b + a_n a^n \implies$$
$$\implies a_n a^n = -a_0 b^n - \ldots - a_{n-1} \cdot a^{n-1} \cdot b \implies$$
$$\implies a_n a^n \cdot \frac{1}{b} = -a_0 b^{n-1} - \ldots - a_{n-1} \cdot a^{n-1} \implies b \mid a_n a^n$$

- Poiché $MCD(a, b) = 1 \implies MCD(a^n, b) = 1$, allora

$$b \mid a_n a^n \implies b \mid a_n$$

- Seguendo gli stessi passaggi, arriviamo a dimostrare che $MCD(a, b) = 1 \implies MCD(a, b^n) = 1$ implica che

$$a \mid a_0 b^n \implies a \mid a_0$$

Esempi:

- Dato $p(x) = x^3 - 19x - 30$, se $\frac{a}{b} \in \mathbb{Q}$ fosse soluzione, allora

$$p\left(\frac{a}{b}\right) \implies a \mid a_0 = 30 \wedge b \mid a_n = 1$$

  quindi le uniche soluzioni possibili di $p(x)$ possono essere:

$$x = \pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30$$

- Dato $p(x) = 6x^3 - 11x^2 + 6x - 1$, se $\frac{a}{b} \in \mathbb{Q}$ fosse soluzione, allora

$$p\left(\frac{a}{b}\right) \implies a \mid a_0 = -1 \wedge b \mid a_n = 6$$

  quindi le uniche soluzioni possibili di $p(x)$ possono essere:

$$x = \pm 1, \pm\frac{1}{2}, \pm\frac{1}{3}, \pm\frac{1}{6}$$

7.3 Polinomi in $\mathbb{Z}_p$

Poiché anche $\mathbb{Z}_p$ è un campo, è possibile trattare anche polinomi a coefficienti in $\mathbb{Z}_p$.

Ad esempio, ricordando che in $\mathbb{Z}_p$ si ha $([a] + [b])^p = [a]^p + [b]^p$, allora

$$(1+x)^p \equiv 1^p + x^p \equiv 1 + x^p (\mathsf{mod}\ n) \implies$$

$$\implies (1+x)^{pn} \equiv (1+x^p)^n (\mathsf{mod}\ n) \implies \sum_{i=0}^{np} \binom{np}{i} x^i \equiv \sum_{i=0}^{n} \binom{n}{j} x^{p(n-j)} (\mathsf{mod}\ n)$$

Corollary 18

Dato $p \in \mathbb{P}$ si ha che:

$$\binom{np}{i} \equiv 0 (\mathsf{mod}\ p) \iff p \nmid i$$

$$\binom{np}{pj} \equiv \binom{n}{j} (\mathsf{mod}\ p)$$

Lemma 53

Dato $p \in \mathbb{P}$, si ha che:

$$\prod_{0<a<p} (x - a) \equiv x^{p-1} - 1 (\mathsf{mod}\ p)$$

Dimostrazione:

- Per il piccolo teorema di Fermat, dato $0 < a < p$ dove $p \in \mathbb{P}$ si ha che:

$$a^{p-1} \equiv 1 (\mathsf{mod}\ p) \implies a^{p-1} - 1 \equiv 0 (\mathsf{mod}\ p)$$

  dunque $[a] \in \mathbb{Z}_p$ è una radice di $q(x) = x^{p-1} - [1] \in \mathbb{Z}_p[x]$

- Siccome $[a]$ è soluzione, allora per il teorema dei fattori si ha che:

$$x-[a] \mid x^{p-1}-[1], \forall 0<a<p \implies \prod_{0<a<p}(x-[a]) \mid x^{p-1}-[1] \implies$$

$$\implies x^{p-1}-[1]=k \cdot \prod_{0<a<p}(x-[a]), \exists k \in \mathbb{Z}$$

- Poiché il coefficiente direttore di $q(x)$ è 1, allora necessariamente si ha che $k=1$, concludendo che:

$$\prod_{0<a<p}(x-a) \equiv x^{p-1}-1 (\mathtt{mod}\ p)$$

Observation 40

Dato $p \in \mathbb{P}$, si ha che:

$$\prod_{0<a<p}(x-a)=\sum_{k=1}^{p}(-1)^{p-k-1}\begin{bmatrix}p\\k\end{bmatrix}x^{k-1}$$

dove $\begin{bmatrix}p\\k\end{bmatrix}$ è un numero di Stirling di prima specie senza segno, ossia il numero di permutazioni in $\mathcal{S}_p$ aventi k cicli

Esempio:

- Dato

$$S_3 : \{(1)(2)(3),(12)(3),(13)(2),(23)(1),(123),(132)\}$$

si ha che:

$$\begin{bmatrix}3\\1\end{bmatrix}=2, \begin{bmatrix}3\\2\end{bmatrix}=3, \begin{bmatrix}3\\3\end{bmatrix}=1$$

Lemma 54

Se $d \mid p-1$, l'equazione $x^d \equiv 1 (\mathtt{mod}\ p)$ ammette d soluzioni distinte in $\mathbb{Z}_p$

Dimostrazione:

- Supponiamo che $d \mid p-1 \implies p-1=dk, \exists k \in \mathbb{Z}$
- Per dimostrazione precedente, sappiamo che

$$\prod_{0<a<p}(x-a) \equiv x^{p-1}-1=x^{nd}-[1]=(x^d-[1])^n=(x^d-[1])\underbrace{(x^d-[1])^{n-1}}_{q(x)}(\mathtt{mod}\ p)$$

- Sempre per dimostrazione precedente, si ha che:

$$x-[a] \mid x^d-[1] \iff [a]^d=[1], \forall 0<a<p$$

oppure che

$$x-[a] \mid q(x)$$

- Per motivi di grado, riapplicando tale procedimento su $q(x)$ e sui suoi fattori, otteniamo esattamente d radici di $x^d - [1]$

Lemma 55

Se $d \mid p-1$, allora $\exists [a] \in \mathbb{Z}_p^* \mid o([a]) = d$

Dimostrazione:

- Se $d = 1$, allora $\exists 1 \in \mathbb{Z}_p^* \mid o([1]) = 1$
- Se $d = q^k$ dove $q \in \mathbb{P}$, allora per il lemma precedente si ha che $x^{q^k} - [1] = [0]$ ha q^k soluzioni.
- Siccome $x^{q^k-1} - [1] = [0]$ ha $q^k - 1$ soluzioni, allora $\exists [a] \in \mathbb{Z}_p^*$ che è soluzione della prima ma non della seconda, implicando che:

$$o([a]) \mid q^k \wedge o([a]) \nmid q^{k-1} \implies o([a]) = q^k$$

- Supponiamo per induzione di aver verificato tale condizione per tutti gli n divisori più piccoli di d.

  Sia quindi $d = nq^k$ dove $q \in \mathbb{P} \mid MCD(n, q^k) = 1$. Per induzione, si ha che:

$$\exists [b], [c] \in \mathbb{Z}_p \mid o([b]) = n, o([c]) = q^k$$

- Come visto nella sezione 4.8, allora

$$MCD(o([b]), o([c])) = 1 \implies \exists a \in \mathbb{Z}_p \mid [a] = [bc] \implies o([a]) = nq^k = d$$

Corollary 19

Dato il gruppo $(\mathbb{Z}_p, \cdot)$ dove $p \in \mathbb{P}$, tale gruppo è sempre ciclico, poiché:

$$p-1 \mid p-1 \implies \exists [a] \in \mathbb{Z}_p^* \mid o([a]) = p-1 = \left|\mathbb{Z}_p^*\right| \iff \mathbb{Z}_p^* = H([a])$$

Capitolo 8

Spazi vettoriali

Definition 57. Spazio vettoriale

Dato un campo K, i cui elementi vengono detti **scalari**, definiamo uno **spazio vettoriale** V, i cui elementi vengono detti **vettori**, sul campo K.

$(V, +)$ è un gruppo abeliano munito di un'operazione aggiuntiva detta **prodotto scalare**

$$\cdot : K \times V \to V : (\lambda, v) \mapsto w$$

la quale rispetta le seguenti proprietà:

- $\forall s, t \in K, v \in V \implies s(t \cdot v) = stv = (s \cdot t)v$ (Associatività)
- $1 \in K, v \in V \implies 1 \cdot v = v$ (Elemento neutro)
- $\forall s, t \in K, v \in V \implies (s + t)v = vs + vt$ (Distributività vettoriale)
- $\forall s \in K, v, w \in V \implies s(v + w) = sv + sw$ (Distributività scalare)

Esempio fondamentale:

- Lo spazio vettoriale $V = K^n = \underbrace{K \times K \times \ldots \times K}_{n \text{ volte}}$ corrisponde a:

$$V = K^n = \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in K\}$$

- Presi dunque due vettori $v, w \in V = K^n$, si ha che

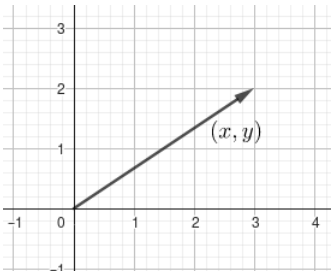
$$\begin{cases} v := (t_1, \ldots, t_n) \in V = K^n \\ w := (s_1, \ldots, s_n) \in V = K^n \end{cases} \implies v + w := (t_1 + s_1, \ldots, t_n + s_n) \in V = K^n$$

- Preso invece uno scalare $\lambda \in K$, si ha che:

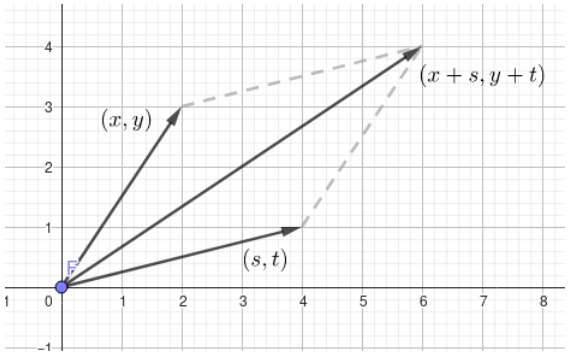
$$\lambda \cdot v = (\lambda t_1, \ldots, \lambda t_n) \in V = K^n$$

Volendo dare un'interpretazione geometrica al tutto, prendiamo come esempio lo spazio vettoriale $\mathbb{R}^2$.

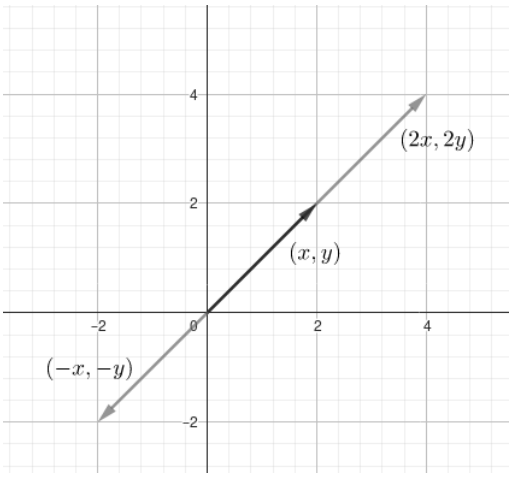
Dato $v := (x, y) \in \mathbb{R}^2$, possiamo rappresentare tale vettore come:



Dato anche $w := (s,t) \in \mathbb{R}^2$, la somma vettoriale $v + w$ corrisponde al *metodo del parallelogramma*:



Dato $\lambda \in \mathbb{R}$, si ha che il vettore $\lambda \cdot v$ ha la stessa direzione del vettore v, ma con lunghezza aumentata o diminuita e verso uguale o invertito



Observation 41

Dato $0_v \in V$, ossia l'elemento neutro di V (detto vettore nullo), e $0 \in K$, ossia l'elemento neutro di K, si ha che:

- $\forall \lambda \in K \implies \lambda \cdot 0_v = 0_v$
- $\forall w \in V \implies 0 \cdot v = 0_v$

8.1 Span e Base

Definition 58. Sottospazio vettoriale

Dato lo spazio vettoriale V definito su K, definiamo $W \subseteq V$ come sottospazio vettoriale di V in K se:

- $(W, +) \subseteq (V, +)$ è un sottogruppo
- $w \in W, \lambda \in K \implies \lambda w \in W$

Esempi:

- $\mathbb{Z}^n \subseteq \mathbb{R}^n$ non è sottospazio vettoriale poiché non verifica la seconda condizione
- $\mathbb{R}^n_{>0} \subseteq \mathbb{R}^n$ non è sottospazio vettoriale poiché non verifica nessuna delle due condizioni

Definition 59. Span

Dato uno spazio vettoriale V su K e dei vettori $v_1, \ldots, v_n \in V$, definiamo **Span** (o sottospazio generato da $v_1, \ldots, v_n$) l'insieme di tutte le **combinazioni lineari** di tali vettori:

$$Span(v_1, \ldots, v_n) : \{\lambda_1 v_1 + \ldots + \lambda_n v_n \mid \lambda_1, \ldots, \lambda_n \in K\}$$

Verifica condizioni per il sottospazio:

- $0_V = 0 \cdot v_1 + \ldots + 0 \cdot v_n \in Span(v_1, \ldots, v_n)$
- $v, w \in Span(v_1, \ldots, v_n) \implies v + w = \lambda_1 v_1 + \ldots + \lambda_n v_n + \mu_1 v_1 + \ldots + \mu_n v_n = (\lambda_1 + \mu_1)v_1 + \ldots + (\lambda_n + \mu_n)v_n \in Span(v_1, \ldots, v_n)$
- $v \in Span(v_1, \ldots, v_n) \implies -v = (-\lambda_1)v_1 + \ldots + (-\lambda_n)v_n \in Span(v_1, \ldots, v_n)$
- $v \in Span(v_1, \ldots, v_n), c \in K \implies cv = (c\lambda_1)v_1 + \ldots + (c\lambda_n)v_n \in Span(v_1, \ldots, v_n)$

Definition 60. Insieme di generatori

Dato uno spazio vettoriale V su K e dei vettori $v_1, \ldots, v_n \in V$, definiamo tali vettori come **insieme di generatori di** V se $V = Span(v_1, \ldots, v_n)$

Definition 61. Indipendenza lineare

Dato uno spazio vettoriale V su K e dei vettori $v_1, \ldots, v_n \neq 0_V \in V$, definiamo tali vettori come **linearmente indipendenti** se

$$\lambda_1 v_1 + \ldots + \lambda_n v_n = 0_V \iff \lambda_1 = \ldots = \lambda_n = 0$$

In caso contrario, vengono detti linearmente dipendenti

Definition 62. Base

Dato uno spazio vettoriale V su K e dei vettori $v_1, \dots, v_n \neq 0_V \in V$, definiamo tali vettori come una **base** se sono un insieme di generatori e linearmente indipendenti

Esempio:

- Dato lo spazio vettoriale $V = K^n$, consideriamo i seguenti vettori $e_1, \dots, e_n \in V$:
  - $e_1 = (1, 0, 0, \dots, 0, 0)$
  - $e_2 = (0, 1, 0, \dots, 0, 0)$
  - $e_3 = (0, 0, 1, \dots, 0, 0)$
  - $\vdots$
  - $e_n = (0, 0, 0, \dots, 0, 1)$
- Tali vettori vengono detto **base canonica di** V, difatti:
  - $e_1, \dots, e_n$ sono generatori di V

    $$v = (t_1, t_2, \dots, t_n) \in V \iff v = (t_1, 0, \dots, 0) + (0, t_2, \dots, 0) + \dots + (0, 0, \dots, t_n) \iff$$
    $$\iff v = t_1 e_1 + t_2 e_2 + \dots + t_n e_n \in Span(e_1, e_2, \dots, e_n)$$
  - $e_1, \dots, e_n$ sono linearmente indipendenti:

    $$\lambda_1 e_1 + \dots + \lambda_n e_n = (0, \dots, 0) \iff (\lambda_1, 0, \dots, 0) + \dots + (0, 0, \dots, \lambda_n) = (0, \dots, 0) \iff$$
    $$(\lambda_1, \lambda_2, \dots, \lambda_n) = (0, \dots, 0) \iff \lambda_1 = \dots = \lambda_n = 0$$

Observation 42

Dato uno spazio vettoriale V su K, i vettori $v_1, \dots, v_n \neq 0_V \in V$ sono linearmente indipendenti se e solo se $v_1, \dots, v_{n-1}$ sono linearmente indipendenti e $v_n \notin Span(v_1, \dots, v_{n-1})$

Dimostrazione (solo in un verso):

- Supponiamo che $v_1, \dots, v_n \neq 0_V \in V$ siano linearmente indipendenti, dunque che

  $$\lambda_1 v_1 + \dots + \lambda_n v_n = 0_V \iff \lambda_1 = \dots = \lambda_n = 0$$
- Se si avesse $\lambda_n \neq 0$, allora

  $$\lambda_1 v_1 + \dots + \lambda_n v_n = 0_V \iff \lambda_1 = \dots = \lambda_n = 0 \implies \lambda_n v_n = -\lambda_1 v_1 - \dots - \lambda_{n-1} v_{n-1} \implies$$
  $$\implies v_n = -\lambda_n^{-1} \lambda_1 v_1 - \dots - \lambda_n^{-1} \lambda_{n-1} v_{n-1} \implies v_n \in Span(v_1, \dots, v_{n-1})$$
- Di conseguenza, si ha che $\lambda_n = 0 \implies v_n \notin Span(v_1, \dots, v_{n-1})$ e che:

  $$\lambda_n = 0 \implies \lambda_1 v_1 + \dots + \lambda_{n-1} v_{n-1} + \lambda_n v_n = 0_V \implies$$
  $$\implies \lambda_1 v_1 + \dots + \lambda_{n-1} v_{n-1} = 0_V \iff \lambda_1 = \dots = \lambda_{n-1} = 0 = \lambda_n$$

Proposition 56

Se i vettori $v_1, \ldots, v_k \in Span(w_1, \ldots, w_n) \subseteq V$ sono linearmente indipendenti, allora $k \leq n$

Dimostrazione:

- Supponiamo $v_1 \neq 0_V \in Span(w_1, \ldots, w_n)$, dunque

$$v = \lambda_1 w_1 + \ldots + \lambda_n w_n \neq 0_V \iff \exists i \in [1, n] \mid \lambda_1 \neq 0$$

- A meno di riordinare i termini, supponiamo $\lambda_1 \neq 0$

$$v = \lambda_1 w_1 + \ldots + \lambda_n w_n \implies \lambda_1 w_1 = v - \lambda_2 w_2 - \ldots - \lambda_n w_n \implies$$

$$\implies w_1 = \lambda_1^{-1} v + (-\lambda_1^{-1}\lambda_2) w_2 - \ldots + (-\lambda_1^{-1}\lambda_n) w_n \implies w_1 \in Span(v_1, w_2, \ldots, w_n)$$

- Poiché $w_1 = \mu_1 v_1 + \mu_2 w_2 + \ldots + \mu_n w_n \in Span(v_1, w_2, \ldots, w_n)$, allora

$$u \in Span(w_1, \ldots, w_n) \implies u = \lambda_1 w_1 + \lambda_2 w_2 + \ldots + \lambda_n v_n =$$

$$= \lambda_1(\mu_1 v_1 + \mu_2 w_2 + \ldots + \mu_n w_n) + \lambda_2 w_2 + \ldots + \lambda_n v_n =$$

$$= (\lambda_1\mu_1) v_1 + (\lambda_1\lambda_2\mu_2) v_2 + \ldots + (\lambda_1\lambda_n\mu_n) v_n \implies u \in Span(v_1, w_2, \ldots, w_n)$$

- Dunque si ha che $Span(w_1, \ldots, w_n) \subseteq Span(v_1, w_2, \ldots, w_n)$. Analogamente, possiamo dimostrare che $Span(v_1, w_2, \ldots, w_n) \subseteq Span(w_1, \ldots, w_n)$, concludendo quindi che $Span(v_1, w_2, \ldots, w_n) = Span(w_1, \ldots, w_n)$
- Supponiamo quindi induttivamente che

$$Span(v_1, \ldots, v_i, w_{i+1}, \ldots, w_n) = Span(w_1, \ldots, w_n)$$

- Dato $v_{i+1} = \mu_1 v_1 + \ldots + \mu_i v_i + \lambda_{i+1} w_{i+1} + \ldots + \lambda_n w_n \in Span(v_1, \ldots, v_i, w_{i+1}, \ldots, w_n)$, se si avesse $(\lambda_{i+1}, \ldots, \lambda_n) = (0, \ldots, 0)$, allora avremmo

$$v_{i+1} = \mu_1 v_1 + \ldots + \mu_i v_i \implies 0_V = (-1) v_{i+1} + \mu_1 v_1 + \ldots + \mu_i v_i$$

  contraddicendo l'ipotesi che $v_1, \ldots, v_k$ siano linearmente indipendenti, dunque l'unica possibilità è

$$v_{i+1} = \mu_1 v_1 + \ldots + \mu_i v_i + \lambda_{i+1} w_{i+1} + \ldots + \lambda_n w_n \neq 0_V \iff \exists j \in [i+1, n] \mid \lambda_j \neq 0$$

- A meno di riordinare i termini, supponiamo $\lambda_{i+1} \neq 0$

$$v_{i+1} = \mu_1 v_1 + \ldots + \mu_i v_i + \lambda_{i+1} w_{i+1} + \ldots + \lambda_n w_n \implies$$

$$\implies \lambda_{i+1} w_{i+1} = v_{i+1} - \mu_1 v_1 - \ldots - \mu_i v_i - \lambda_{i+2} w_{i+2} - \ldots - \lambda_n w_n \implies$$

$$w_{i+1} = \lambda_{i+1}^{-1} v_{i+1} + (-\lambda_{i+1}^{-1}\mu_1) v_1 + \ldots + (-\lambda_{i+1}^{-1}\mu_i) v_i + (-\lambda_{i+1}^{-1}\lambda_{i+2}) w_{i+2} + \ldots + (-\lambda_{i+1}^{-1}\lambda_n) w_n$$

$$\implies w_{i+1} \in Span(v_1, \ldots, v_i, v_{i+1}, w_{i+2}, \ldots, w_n)$$

- Dunque si ha che

$$Span(v_1, \dots, v_i, w_{i+1}, w_{i+2}, \dots, w_n) \subseteq Span(v_1, \dots, v_i, v_{i+1}, w_{i+2}, \dots, w_n)$$

.

Analogamente, possiamo dimostrare che

$$Span(v_1, \dots, v_i, v_{i+1}, w_{i+2}, \dots, w_n) \subseteq Span(v_1, \dots, v_i, w_{i+1}, w_{i+2}, \dots, w_n)$$

concludendo quindi che

$$Span(v_1, \dots, v_i, v_{i+1}, w_{i+2}, \dots, w_n) = Span(v_1, \dots, v_i, w_{i+1}, w_{i+2}, \dots, w_n)$$

e quindi, per induzione, che $Span(v_1, \dots, v_n) = Span(w_1, \dots, w_n)$

- Se per assurdo si avesse che $k > n$, allora

$$v_{n+1} \in Span(w_1, \dots, w_n) = Span(v_1, \dots, v_n)$$

contraddicendo l'ipotesi che $v_1, \dots, v_k$ siano indipendenti.

Corollary 20

Siano $v_1, \dots, v_n \in V$ e $w_1, \dots, w_m \in V$ due basi di V. In tal caso, si ha che $n = m$, ossia hanno la stessa **cardinalità**

Dimostrazione:

- Siccome sono entrambi basi, si ha che

$$Span(v_1, \dots, v_n) = V = Span(w_1, \dots, w_m)$$

- Di conseguenza, poiché i vettori $v_1, \dots, v_n \in V = Span(w_1, \dots, w_m)$ sono linearmente indipendenti, allora $n \leq m$
- Analogamente, poiché i vettori $w_1, \dots, w_m \in V = Span(v_1, \dots, v_m)$ sono linearmente indipendenti, allora $m \leq n$
- Dunque, l'unica possibilità è che $n = m$

Definition 63. Dimensione di uno spazio vettoriale

Dato uno spazio vettoriale V su K, definiamo come **dimensione di** V ($dim(V)$) la cardinalità di una sua base

Esempio:

- Data la base canonica di K^n, ossia $e_1, \dots, e_n$, si ha che:

$$dim(K^n) = n$$

Observation 43

I vettori $v_1, \ldots, v_n \in V$ sono una base di V se e solo se

$$\forall v \in V, \exists! \lambda_1, \ldots, \lambda_n \mid v = \lambda_1 v_1 + \ldots + \lambda_n v_n$$

Inoltre, chiamiamo tali unici scalari come **coordinate di v in tale base**

Dimostrazione:

- Se $v_1, \ldots, v_n \in V$ sono una base di V, in quanto generatori di V si ha che ogni vettore $v \in V$ può essere espresso come una combinazione lineare di $v_1, \ldots, v_n$.
- Supponiamo ora che esistano due combinazioni lineari tali che

$$\mu_1 v_1 + \ldots + \mu_n v_n = v = \lambda_1 v_1 + \ldots + \lambda_n v_n$$

- In tal caso si ha che

$$\mu_1 v_1 + \ldots + \mu_n v_n = \lambda_1 v_1 + \ldots + \lambda_n v_n \implies \mu_1 v_1 + \ldots + \mu_n v_n - \lambda_1 v_1 - \ldots - \lambda_n v_n = 0_V \implies$$

$$\implies (\lambda_1 - \mu_1) v_1 + \ldots + (\lambda_n - \mu_n) v_n = 0_V$$

- Poiché $v_1, \ldots, v_n$ sono linearmente indipendenti, si ha che:

$$(\lambda_1 - \mu_1) v_1 + \ldots + (\lambda_n - \mu_n) v_n = 0_V \iff (\lambda_1 - \mu_1) = \ldots = (\lambda_n - \mu_n) = 0$$

implicando quindi che

$$\lambda_1 = \mu_1, \ldots, \lambda_n = \mu_n$$

Observation 44

Diciamo che V ha dimensione infinita se non esiste un insieme finito di generatori

Esempi:

- Lo spazio vettoriale V definito su $K[x]$ non può avere base finita: dati $p_1(x), \ldots, p_n(x) \in V$ e $\lambda_1, \ldots, \lambda_n \in K$ si ha che:

$$deg(\lambda_1 p_1(x) + \ldots + \lambda_n p_n(x) \leq max(deg(p_1(x)), \ldots, deg(p_n(x)))$$

Infatti, in tale esempio la base è data dai monomi $1, x, x^2, \ldots$

- Lo spazio vettoriale V definito su $K^S : \{f : S \to K\}$ ha dimensione finita se e solo se S ha cardinalità finita

8.2 Trasformazioni lineari

Definition 64. Trasformazione lineare

Dati due spazi vettoriali V e W definiti sullo stesso campo K, la funzione $f : V \to W$ viene detta **trasformazione lineare** (o morfismo tra spazi vettoriali) se:

- $\forall v, v' \in V, f(v + v') = f(v) + f(v')$
- $\forall \lambda \in K, v \in V, f(\lambda v) = \lambda f(v)$

Theorem 57

Dato uno spazio vettoriale V si ha che:

$$dim(V) = n \implies V \cong K^n$$

Dimostrazione:

- Siano $v_1, \ldots, v_n$ una base di V (dunque $dim(V) = n$). Definiamo la funzione

$$f : K^n \to V : (t_1, \ldots, t_n) \mapsto (t_1 v_1 + \ldots + t_n v_n)$$

- Poiché $\forall v \in V, \exists! \lambda_1, \ldots, \lambda_n \mid v = \lambda_1 v_1 + \ldots + \lambda_n v_n$, la funzione f è automaticamente biettiva:

$$\left.\begin{array}{r} v_1, \ldots, v_n \text{ generatori di } V \implies f \text{ suriettiva} \\ v_1, \ldots, v_n \text{ lin. indipendenti} \implies f \text{ iniettiva} \end{array}\right\} \implies f \text{ biettiva}$$

- Dati quindi $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in K^n$, si ha che:

$$f(x+y) = (x_1+y_1)v_1+\ldots+(x_n+y_n)v_n = x_1v_1+\ldots+x_nv_n+y_1v_1+\ldots+y_nv_n = f(x)+f(y)$$

- Dato invece $\lambda \in K$, si ha che:

$$f(\lambda v) = \lambda x_1 v_1 + \ldots \lambda x_n v_n = \lambda(x_1 v_1 + \ldots + x_n v_n) = \lambda f(x)$$

- Dunque, concludiamo che f sia un isomorfismo, implicando che anche f^{-1} lo sia.

$$V \cong K^n$$

Theorem 58

Dati due spazi vettoriali V e W definiti sullo stesso K, si ha che:

$$V \cong W \iff dim(V) = dim(W)$$

Dimostrazione:

- $dim(V) = dim(W) \implies V \cong W$
  - Sappiamo già che $dim(V) = dim(W) = n \implies V \cong K^n \cong W$
- $V \cong W \implies dim(V) = dim(W)$
  - Supponiamo che $V \cong W$, dove f è l'isomorfismo, e sia $v_1, \ldots, v_n$ una base di V.
  - Siccome f è suriettiva si ha che $\forall w \in W, \exists v \in V \mid w = f(v)$, dunque si ha che

    $$w = f(v) = f(\lambda_1 v_1 + \ldots + \lambda_n v_n = \lambda_1 f(v_1) + \ldots + \lambda_n f(v_n) \in Span(f(v_1), \ldots, f(v_n))$$

    Dunque $f(v_1), \ldots, f(v_n)$ sono generatori di W
  - Siccome f è un morfismo, si ha che

    $$f(0_V) = 0_W = \lambda_1 f(v_1) + \ldots + \lambda_n f(v_n) = f(\lambda_1 v_1 + \ldots + \lambda_n v_n)$$

  - Siccome f è suriettiva, allora

    $$f(0_V) = f(\lambda_1 v_1 + \ldots + \lambda_n v_n) \iff 0_V = \lambda_1 v_1 + \ldots + \lambda_n v_n$$

  - Siccome $v_1, \ldots, v_n$ sono linearmente indipendenti, allora

    $$0_V = \lambda_1 v_1 + \ldots + \lambda_n v_n \iff \lambda_1 = \ldots = \lambda_n = 0$$

    implicando quindi che anche $f(v_1), \ldots, f(v_1)$ siano linearmente indipendenti

    $$0_W = \lambda_1 f(v_1) + \ldots + \lambda_n f(v_n) \iff \lambda_1 = \ldots = \lambda_n = 0$$

  - I vettori $f(v_1), \ldots, f(v_n)$ sono quindi una base di W,la cui dimensione corrisponde a quella di V

Definition 65. Spazio quoziente

Dato uno spazio vettoriale V e un sottospazio $W \subseteq V$, lo **spazio quoziente** V/W è uno spazio vettoriale con la somma $[v] + [v'] = [v + v']$ e il prodotto scalare $\lambda[x] = [\lambda x]$

Dimostrazione:

- La dimostrazione della ben definizione della somma è analoga a quella del normale gruppo quoziente
- Dimostriamo quindi che il prodotto scalare sia ben definito

$$[v] = [v'] \implies v' - v \in W \implies \lambda(v' - v) = \lambda v' - \lambda v \in W \implies [\lambda v] = [\lambda v']$$

Theorem 59. Dimensione spazio quoziente

Dato uno spazio vettoriale V e un sottospazio $W \subseteq V$, si verifica che

$$dim(V/W) = dim(V) - dim(W)$$

Dimostrazione:

- Sia $w_1, \ldots, w_k$ una base di W. Se $dim(V) > k$ allora $Span(w_1, \ldots, w_k) \subsetneqq V$.
- Di conseguenza, esiste $v_{k+1} \in V \mid v_{k+1} \notin Span(w_1, \ldots, w_k)$, implicando che $w_1, \ldots, w_k, v_{k+1}$ siano linearmente indipendenti
- A questo punto, se $dim(V) > k+1$, allora esiste $v_{k+2} \in V \mid v_{k+2} \notin Span(w_1, \ldots, w_k, v_{k+1})$, implicando che $w_1, \ldots, w_k, v_{k+1}, v_{k+2}$ siano linearmente indipendenti
- Ripetendo tale procedimento $n-k = dim(V) - dim(W)$ volte arriviamo a costruire una base di V della forma $w_1, \ldots, w_k, v_{k+1}, \ldots, v_n$
- Dato $v \in Span(w_1, \ldots, w_k, v_{k+1}, \ldots, v_n)$, si ha che:

$$v = \lambda_1 w_1 + \ldots + \lambda_k w_k + \lambda_{k+1} v_{k+1} + \ldots + \lambda_n v_n \implies$$
$$\implies [v] = \lambda_1 [w_1] + \ldots + \lambda_k [w_k] + \lambda_{k+1} [v_{k+1}] + \ldots + \lambda_n [v_n]$$

- Notiamo come

$$w_1, \ldots, w_k \in W \implies 0_V - w_1, \ldots, 0_V - w_k \in W \implies$$
$$\implies w_1 \sim 0_V, \ldots, w_k \sim 0_V \implies [0_V] = [w_1] = \ldots = [w_k]$$

- Di conseguenza, si ha che $[v_{k+1}], \ldots, [v_n]$ sono generatori di V/K

$$[v] = \lambda_1 [w_1] + \ldots + \lambda_k [w_k] + \lambda_{k+1} [v_{k+1}] + \ldots + \lambda_n [v_n] \implies$$
$$\implies [v] = \lambda_1 [0_V] + \ldots + \lambda_k [0_V] + \lambda_{k+1} [v_{k+1}] + \ldots + \lambda_n [v_n] = \lambda_{k+1} [v_{k+1}] + \ldots + \lambda_n [v_n]$$

- Supponiamo quindi $[0_V] \in V/W$ possa essere scritto come una combinazione lineare di V/W:

$$[0_V] = \lambda_{k+1} [v_{k+1}] + \ldots + \lambda_n [v_n] \implies$$
$$\implies [0_V] = [\lambda_{k+1} v_{k+1} + \ldots + \lambda_n v_n] \implies$$

- Poiché $\lambda_{k+1} v_{k+1} + \ldots + \lambda_n v_n \in W$, si ha che

$$\lambda_{k+1} v_{k+1} + \ldots + \lambda_n v_n = \lambda_1 w_1 + \ldots + \lambda_k w_k \implies$$
$$\lambda_{k+1} v_{k+1} + \ldots + \lambda_n v_n - \lambda_1 w_1 - \ldots - \lambda_k w_k = 0_V$$

- Poiché $w_1, \ldots, w_k, v_{k+1}, \ldots, v_n$ sono linearmente indipendenti, allora

  $$\lambda_{k+1} v_{k+1} + \ldots + \lambda_n v_n - \lambda_1 w_1 - \ldots - \lambda_k w_k = 0_V \iff \lambda_1 = \ldots = \lambda_k = \lambda_{k+1} = \ldots = \lambda_n = 0$$

  implicando quindi che anche $\lambda_{k+1} v_{k+1} + \ldots + \lambda_n v_n$ siano linearmente indipendenti, rendendoli una base di V/W, la cui dimensione è $n - k = dim(V) - dim(W)$

Proposition 60

Dati due spazi vettoriali V e W e una trasformazione lineare $f : V \to W$, il nucleo $Ker(f) \subseteq V$ e l'immagine $Im(f) \subseteq W$ di f sono definiti come

$$Ker(f) : \{v \in V \mid f(v)0_W\}$$

$$Im(f) : \{w \mid w = f(v)\exists v \in V\}$$

I quali sono entrambi sottospazi vettoriali, rispettivamente di V e W

Dimostrazione:

- Sappiamo già che essi sono sottogruppi per la somma
- Verifichiamo quindi che siano chiusi nel prodotto scalare

$$v \in Ker(f), \lambda \in K \implies f(\lambda v) = \lambda f(v) = \lambda 0_W = 0_W \implies \lambda v \in Ker(f)$$

$$w = f(v) \in Im(f), \lambda \in K \implies \lambda w = \lambda f(v) = f(\lambda v) \implies \lambda v \in Im(f)$$

Observation 45. Teorema fondamentale di isomorfismo

Data una trasformazione lineare $f : V \to W$, si ha che

$$V/Ker(f) \cong Im(f)$$

Implicando anche che $dim(V/Ker(f)) = dim(Im(f))$

Theorem 61. Teorema del Rango

Data una trasformazione lineare $f : V \to M$, definiamo come **rango di** f la dimensione della sua immagine:

$$rk(f) := dim(Im(f)) = dim(V/Ker(f)) = dim(V) - dim(Ker(f))$$