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

13 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

Algebra elementare

1.1 Richiami di insiemistica

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

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

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

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

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

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

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

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

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

- 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

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

- Una funzione viene detta **iniettiva** se <u>ogni</u> 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 <u>ogni</u> 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

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

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

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

- 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 Assiomi, Strutture algebriche e Gruppi

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 presi due elementi di S in input, restituisce un elemento di S in output

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

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:

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

Tali operazioni binarie **possono** godere di alcune **proprietà algebriche**:

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

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

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

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

Tale assioma implica necessariamente l'esistenza dell'elemento neutro e

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. Se valgono gli assiomi di **elemento neutro** e di **commutatività**, allora 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. Se vale l'assioma di **elemento inverso**, allora può esistere **un solo elemento inverso**:
$$m(x, x_1^{-1}) = 1 = m(x, x_2^{-1}) \implies m(x, x_1^{-1}) = m(x, x_2^{-1}) \implies x_1^{-1} = x_2^{-1}$$

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:
$$f, g, h : X \to X \implies h \circ (g \circ f) = (h \circ g) \circ f \implies \texttt{Associatività}$$
$$f : X \to X : x \to f(x), \texttt{idt} : X \to X : x \to x \implies f \circ \texttt{idt} = f \implies \texttt{Elemento neutro}$$
dove `idt` è la funzione identità, ossia $idt(x) = x$.

- Dato un insieme X, denotiamo con S_X il **gruppo simmetrico su X**, ossia l'insieme composto da tutte le funzioni biettive da X in se stesso.

$$S_X : \{f : X \to X \,|\, f \texttt{ è biettiva}\}$$

Allora, la coppia $(S_X, \circ)$ è un gruppo, poiché:

$$f, g, h : X \to X \implies h \circ (g \circ f) = (h \circ g) \circ f \implies \texttt{Associatività}$$
$$f : X \to X : x \to f(x), \texttt{idt} : X \to X : x \to x \implies f \circ \texttt{idt} = f \implies \texttt{Elemento neutro}$$
$$\exists f^{-1} : X \to X \,|\, f \circ f^{-1} = \texttt{idt} \implies \texttt{Elemento inverso}$$

Observation 2

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
$$\forall x \in X, \exists! y \,|\, f(y) = x$$

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

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

1.2.1 Approfondimento sul gruppo simmetrico

Avendo introdotto il gruppo simmetrico su X come

$$S_X : \{f : X \to X \,|\, f \texttt{ è biettiva}\}$$

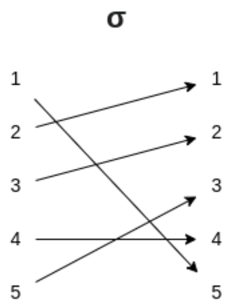
Tale insieme presenta alcune caratteristiche:

- 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 S_n
- Poiché tutte le permutazioni possibili di un insieme di n elementi corrispondono a $n!$, allora abbiamo che $|X| = n \implies |S_n| = n!$

Data una **permutazione** $\sigma \in S_n$, possiamo utilizzare due notazioni per poterne descrivere il comportamento:

Tramite grafo

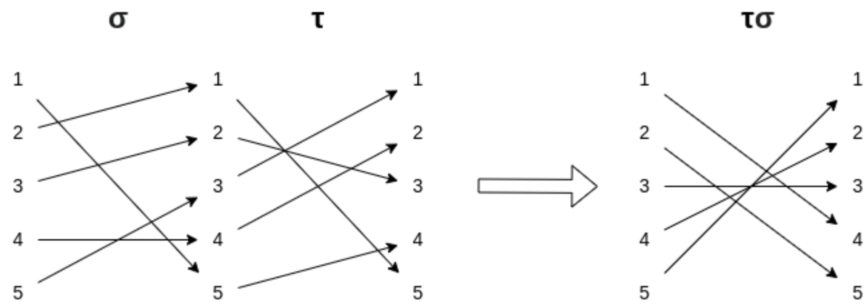


Tramite matrice

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

Possiamo definire l'**operazione prodotto tra due permutazioni** come l'applicazione susseguita di entrambe le permutazioni. Ad esempio, consideriamo il prodotto $\sigma \cdot \sigma$, dove σ è la permutazione descritta nell'esempio precedente. In tal caso, si ha che:

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



- 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):

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

Attenzione:

È necessario evidenziare come l'operazione prodotto tra due permutazioni **non sia commutativa** se le due permutazioni sono diverse tra loro, dunque $\tau\sigma \neq \sigma\tau$

1.3 Anelli e Campi

Consideriamo un insieme A e due operazioni binarie su di esso, 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 **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 3

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 stesso 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, poniamo:

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

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

$$0 = a \cdot 0$$

Nel caso in cui si abbia un **anello commutativo** in cui viene rispettato l'assioma di **elemento inverso** nell'operazione prodotto, allora definiamo tale struttura algebrica come **campo**.

Definition 8. Campo

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

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

$$\forall a \in A \setminus \{0\}, \exists a^{-1} \in A \,|\, a \cdot a^{-1} = 1$$

Dunque, in un campo si ha anche che $(A \setminus \{0\}, \cdot)$ è un gruppo abeliano

Esempi:

- $(\mathbb{Z}, +, \cdot)$ è un **anello commutativo**
- $(\mathbb{Q}, +, \cdot)$ è un **campo**
- $(\mathbb{R}, +, \cdot)$ è un **campo**
- Sia A un **anello commutativo**. Definiamo l'**insieme dei polinomi** aventi come coefficienti elementi dell'anello A come:

  $A[x] : \{\texttt{polinomi a coefficienti in } A\} : \{a_0 + a_1x + ... + a_nx^n \,|\, a_0, a_1, ..., a_n \in A\}$

  Dati due polinomi $p(x), q(x) \in A[x]$, dunque definiti come

  $$p(x) = \sum_{i=0}^{n} a_ix^i \qquad q(x) = \sum_{i=0}^{n} b_ix^i$$

  abbiamo che:

  - L'**operazione somma** corrisponde a:

    $$p(x) + q(x) = \sum_{i=0}^{+\infty} (a_i + b_i)x^i$$

    dove $a_i, b_i = 0$ per $i > n$
  - L'**operazione prodotto** corrisponde a:

    $$p(x) \cdot q(x) = \sum_{i=0}^{n} \left(\sum_{j=0}^{n} a_ib_jx^{i+j} \right)$$

  - In $(A[x], +, \cdot)$ l'**elemento neutro** è il polinomio costante (ossia aventi solo grado zero), indicato col simbolo 1

– Poiché possiamo vedere ogni $a \in A$ come un **polinomio costante** in $A[x]$ (dunque un polinomio del tipo $p(x) = a_0 + a_1x^0 ... + a_nx^0 \in A[x] \,|\, a_0 \in A$), allora deduciamo che $A \subset A[x]$, implicando che $(A[x], +, \cdot)$ possa essere un anello commutativo se e solo se anche A lo è, fattore dato per vero come ipotesi iniziale.

– Tuttavia, l'anello commutativo $(A[x], +, \cdot)$ **non ammette elemento inverso nell'operazione prodotto**, poiché il grado dei polinomi è $0 \leq i \leq n$. Ad esempio, il polinomio $p(x) = x$ non ammette inversi, poiché $x^{-1} \notin A[x]$. Dunque, $(A, +, \cdot)$ **non è un campo**.

1.3.1 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

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

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 $\mathbb{R} \subset \mathbb{C}$, poiché $\forall a \in \mathbb{R} \implies z \in \mathbb{C} \,|\, z = a + i \cdot 0$. Inoltre, definiamo un **numero immaginario puro** come un numero nella forma $z \in \mathbb{C} \,|\, z = 0 + i \cdot b$.

In questa sezione, vedremo le varie **proprietà dei numeri complessi**, arrivando fino al provare che essi corrispondano ad un **campo**.

Partiamo dal definire le operazioni di somma e prodotto. Dati due numeri $z, w \in \mathbb{C}$, definiti come $z = a + ib$ e $w = c + id$, abbiamo che:

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

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

Verifichiamo facilmente che la struttura $(\mathbb{C}, +, \cdot)$ risulta essere un **anello commutativo**:

- **Associatività della somma**

$$(z + w) + q = z + (w + q) = z + w + q, \quad \forall z, w, q$$

- **Elemento neutro della somma**

$$\exists! 0 \in \mathbb{C} \,|\, z + 0 = z, \quad \forall z \in \mathbb{C}$$

- **Elemento inverso della somma**

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

- **Commutatività della somma**

$$\forall z, w \in \mathbb{C} \,|\, z + w = w + z$$

- **Associatività del prodotto**

$$(zw)q = z(wq) = zwq, \quad \forall z, w, q$$

- **Elemento neutro del prodotto**

$$\exists 1 \in \mathbb{C} \,|\, z \cdot 1 = z, \quad \forall z \in \mathbb{C}$$

- **Commutatività del prodotto**

$$\forall z, w \in \mathbb{C} \,|\, zw = wz$$

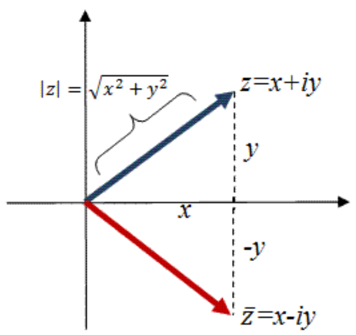
- **Relazione distributiva**

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

A questo punto, l'ultimo step da svolgere per poter definire $(\mathbb{C}, +, \cdot)$ come un **campo**, ossia provare l'ammissione dell'**assioma di elemento inverso del prodotto**.

Poiché un numero complesso è determinato da una **coppia di valori** $a, b \in \mathbb{R} \,|\, z \in \mathbb{C}, z = a + ib$, 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**.

Ad esempio, il numero $z = -3 - 3i$ viene rappresentato come:



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**:

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

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

$$z = a + ib \implies \overline{z} = a - ib \implies Im(\overline{z}) = -Im(z)$$

Observation 4

- Dati $z, w \in \mathbb{C} \,|\, z = a + ib, w = c + id$, 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 $z, w \in \mathbb{C} \,|\, z = a + ib, w = c + id$, 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

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

A questo punto, proviamo a definire l'elemento inverso del prodotto come:

$$\forall z \in \mathbb{C} \setminus \{0\}, \exists! z^{-1} = \frac{1}{z} = \frac{1}{a + ib} \,|\, z \cdot z^{-1} = 1$$

Tuttavia, il numero inverso $z^{-1} = \frac{1}{a+ib}$ non risulta apparire nella forma $c + id \,|\, c, d \in \mathbb{R}$. Decidiamo quindi di riscrivere z^{-1} come:

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

A questo punto, ponendo $c = \frac{a}{a^2+b^2}$ e $d = \frac{-b}{a^2+b^2}$, otteniamo che $z^{-1} = c + id \implies z^{-1} \in \mathbb{C}$ è un numero complesso diverso da zero, rispettando il vincolo di dominio richiesto dalla condizione di validità dell'assioma di elemento inverso del prodotto.

Avendo provato quindi la validità dell'ultimo assioma richiesto, possiamo dichiarare i **numeri complessi** come un **campo**.

Approfondimento sui numeri complessi

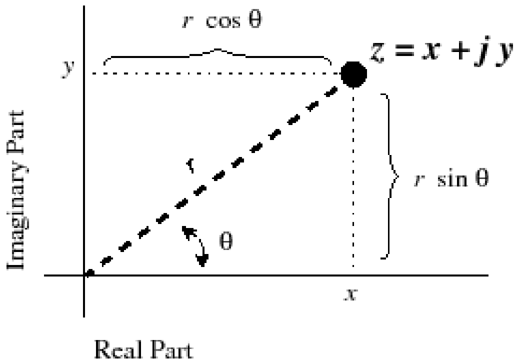
Abbiamo visto come un numero complesso possa essere espresso come un punto sul piano gaussiano tramite una **coppia di valori**, descrivendo la distanza di tale punto dall'origine del piano $(0, 0)$ come $|z|$.

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:

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

Introduciamo ora la seguente **notazione contratta**:

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

Riscriviamo quindi la forma polare di z come:

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

Giustificazione:

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, riscriviamo tale espressione come:

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

Riscrivendo il risultato nella forma contratta imposta, 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**:

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

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 $z^1 0$ come:

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

1.3.2 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 $k = 0, 1, ..., n-1$ 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 $k = 2$
$$x_3 = e^{i(\frac{1}{2\cdot 3}\pi + \frac{4\pi}{3})} = e^{\frac{9}{6}\pi i} = e^{\frac{3}{2}\pi i}$$

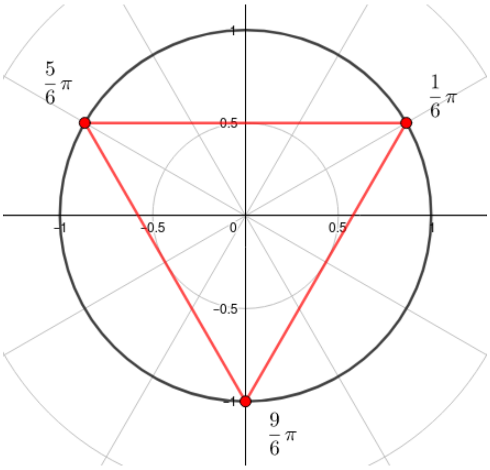
- Se $k = 3$
$$x_4 = e^{i(\frac{1}{2\cdot 3}\pi + \frac{6\pi}{3})} = e^{i(\frac{1}{6}\pi + 2\pi)} = e^{\frac{1}{6}\pi i} \implies x_4 = x_1$$

- 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 5

Le n radici n-esime di un numero complesso sono i 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**

Definition 9. Teorema fondamentale dell'algebra

Data un'equazione del tipo:

$$(E) = a_0 + a_1 x + ... + a_n x^n$$

dove (E) indica una qualsiasi espressione e $a_i \in \mathbb{C}, n \geq 1, a_n \neq 0$, **esiste sempre almeno una soluzione complessa di** (E).

1.4 Relazioni

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

$$R \subseteq S \times S \implies R \subset \{(x, y) \,|\, x, y \in S\}$$

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

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

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

- **Riflessività**:
$$xRx \quad \forall x \in S$$
- **Simmetria**:
$$xRy \implies yRx \quad \forall x, y \in S$$
- **Anti-simmetria**:
$$xRy \land yRx \implies x = y \quad \forall x, y \in S$$
- **Transitività**:
$$xRy \land yRz \implies xRz \quad \forall x, y, z \in S$$

Una relazione viene detta **relazione di equivalenza** se su di essa valgono le proprietà di riflessività, simmetria e transitività. L'esempio più banale tale relazione è la relazione di uguaglianza, indicata col simbolo $=$.

Una relazione viene detta **relazione d'ordine parziale** se su di essa valgono le proprietà di riflessività, anti-simmetria e transitività. L'esempio più banale tale relazione è la relazione di precedenza, indicata col simbolo $\prec$. Nel caso in cui tutti gli elementi di una relazione d'ordine parziale siano confrontabili tra di loro (ossia se $\forall x, y \in S$ vale $xRy \lor yRx$), definiamo tale relazione come **relazione d'ordine totale**.

Esempi:

- La relazione $\leq$ è un 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):
  $$A \subseteq B \land B \subseteq A \implies A = B$$
  - Se un sottoinsieme A è sottoinsieme di B e B è sottoinsieme di C, allora anche A è sottoinsieme di C (transitività):
  $$A \subseteq B \land B \subseteq C \implies A \subseteq C$$
  - Non tutti i sottoinsiemi sono confrontabili tra loro (ordine non totale), ad esempio $\{1\} \not\subseteq \{2\}$

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

$$| \; : \{(m, n) \,|\, m, n \in \mathbb{Z}, \exists p \in \mathbb{Z}, m \cdot p = n\}$$

Analizziamo le proprietà della relazione definita:

  - Soddisfa la **riflessività**:

$$m \,|\, m \quad \forall m \in \mathbb{Z} \implies m \cdot 1 = m$$

  - Soddisfa la **transitività**:

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

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

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

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

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

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

$$m \,|\, n \wedge n \,|\, m \implies m = n \cdot q = m \cdot p \cdot q$$

  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 $|$ 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.

1.4.1 Relazione di congruenza

Un particolare esempio di relazione di equivalenza è la **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 vale n è divisore di $b - a$ $(n \,|\, b - a)$.

Esempi:

- $7 \equiv 22 (\texttt{mod}\ 5) \implies b - a = 22 - 7 = 15\%5 = 0$
- $7 \equiv 13 (\texttt{mod}\ 5) \implies b - a = 13 - 7 = 6\%5 = 1$

La relazione definita risulta essere:

- **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**:

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

- **Transitiva**:

  Siccome:

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

  allora:

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

1.4.2 Teorema della divisione con resto euclidea

Theorem 1. 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 $m(\texttt{mod}\ n)$:

$$[m] : \{a \in \mathbb{Z} \,|\, a \equiv m(\texttt{mod} n)\}$$

Allora, abbiamo che:

$$n \,|\, m - a \implies m - a = n \cdot p \implies a = m - np$$

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

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

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:

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

1.4.3 Classi di equivalenza

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

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

Ogni classe di equivalenza possiede **almeno un elemento**, poiché $x \sim x, \forall x \in S$ per riflessività della relazione d'equivalenza. Inoltre, per transitività abbiamo che:

- Avendo $x \sim y$, 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 $z \in [x] \land z \in [y] \implies z \sim x \land z \sim y$, dunque per transitività si verifica che $x \sim y$. Dunque, concludiamo che:

$$x \nsim y \iff [x] \cap [y] = \emptyset$$

Da tali implicazioni, otteniamo che le **classi di equivalenza** indotte da una relazione su un insieme X sono **tutte disgiunte tra loro**.

Indichiamo quindi l'insieme di tutte le classi di equivalenza di un insieme X indotte da una relazione di equivalenza come:

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

Dato un insieme X e un insieme I contenente degli indici, una **partizione di** X è un sottoinsieme di X disgiunto da tutte le altre partizioni di X:

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

Per comodità, denotiamo il partizionamento di un insieme X come

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

In particolare, è opportuno puntualizzare come **applicare una relazione di equivalenza su un insieme equivale a partizionare tale insieme**, dove ogni classe di equivalenza corrisponde ad una partizione dell'insieme:

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

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

- **Riflessività**:
$$\forall x \in X, \exists i \in I \,|\, x \in X_i \implies x \sim x$$

- **Simmetria**:
$$x \sim y, \exists i, j \in I \,|\, x, y \in X_i \implies x, y \in X_j \implies y \sim x$$

- **Transitività**:
$$x \sim y, y \sim z, \exists i, j \in I \,|\, x, y \in X_i, y, z \in X_j \implies y \in X_i \cap X_j$$

  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 $x \sim z$.

Infine, affermiamo che applicare una relazione di equivalenza su un insieme equivale all'applicazione di una **funzione suriettiva** detta **proiezione al quoziente**, la quale mappa ogni elemento x alla sua classe di equivalenza di appartenenza:

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

Capitolo 2

Elementi di teoria dei gruppi

2.1 Sottogruppi

Definition 10. Sottogruppo

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

- $e \in H$, dove e è l'elemento neutro di G
- $x, y \in H \implies xy \in H$ (dunque chiusa nell'operazione)
- $x \in H \implies x^{-1} \in H$ (dunque chiusa nell'operazione)

Esempio:

- $(\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +) \subset (\mathbb{C}, +)$
- $(\mathbb{Z} \setminus \{0\}, \cdot) \not\subset (\mathbb{Q} \setminus \{0\}, \cdot) \subset (\mathbb{R} \setminus \{0\}, \cdot)$
- Sia A un anello. Dato $a \in A$, definiamo come $I(a)$ l'**insieme dei multipli** di a:

$$I(a) : \{ax \,|\, x \in A\}$$

  Verifichiamo che $(I(a), +) \subset (A, +)$, ricordando che $(A, +)$ è un gruppo abeliano poiché A è un anello:

  - $0 = a \cdot 0$, dunque $0 \in I(a)$
  - $x, y \in I(a) \implies \exists b, c \in A \,|\, x = ab, y = ac \implies x + y = ab + ac = a(b + c) \implies x + y \in I(a)$
  - $x \in I(a) \implies \exists b \in A \,|\, x = ab \implies -x = a(-b) \implies -x \in I(a)$

2.1.1 Classi laterali sinistre e Teorema di Lagrange

Sia $(G, \cdot)$ un gruppo e sia $H \subset G$ 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 11. Classi laterali sinistre

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

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

Denotiamo come G/H il gruppo di tutte delle classi di equivalenza di G indotte da tale relazione, corrispondente quindi all'insieme di tutte le classi laterali sinistre.

Observation 6

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

Tale particolare gruppo quoziente viene indicato come $\mathbb{Z}_n$

$$\mathbb{Z}_n := Z/I(n) = Z/\equiv$$

Dimostrazione:

- Abbiamo già dimostrato che $I(n) \subset \mathbb{Z}$ è sottogruppo
- Applicando la relazione $x \sim y \iff x^{-1}y \in H$, in tal caso otteniamo che:
$$a \sim b \implies (-a) + b = b - a \in I(n) \implies \exists k \in \mathbb{Z} \,|\, b - a = nk \implies$$
$$\implies n \,|\, b - a \implies a \equiv b (\mathtt{mod} \;\; n)$$
- Procedendo all'inverso, otteniamo che $a \equiv b(\mathtt{mod} \;\; n) \implies a \sim b$

Observation 7

Ogni classe laterale sinistra ($\forall[x] \in G/H$) coincide anche a:

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

Dimostrazione:

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

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

  Allora abbiamo che:

$$\begin{aligned} h &= x^{-1}y \\ xh &= x(x^{-1}y) \\ xh &= y \end{aligned}$$

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

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

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

  Allora abbiamo che:

$$\begin{aligned} y &= xh \\ x^{-1}y &= x^{-1}(xh) \\ x^{-1}y &= h \end{aligned}$$

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

Observation 8

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 $\varphi : H \to xH : h \mapsto xh$ 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:

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

Theorem 2. Teorema di Lagrange

Sia G un **gruppo finito** e sia $H \subset G$ 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:

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

2.1.2 Operazioni su gruppo quoziente

Proposition 3

Sia $(G, +)$ un **gruppo abeliano** e sia $H \subset G$ **sottogruppo**. In tal caso, anche $(G/H, +)$ 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**:

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

- Considerando, ad esempio, il gruppo abeliano $(\mathbb{Z}, +)$ e il suo sottogruppo $(I(n), +)$, otteniamo che anche **il gruppo quoziente** $\mathbb{Z}_n = \mathbb{Z}/I(n)$ **è abeliano**.

  Ad esempio, in $\mathbb{Z}_{11}$ si avrà che:

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

2.2 Ideali

Definition 12. Ideale

Sia $(A, +, \cdot)$ un anello commutativo. Definiamo $I \subset A$ come l'**ideale** di A se si verifica che:

- $(I, +) \subset (A, +)$, ossia se è un sottogruppo dell'anello per la somma
- $x \in I, a \in A \implies ax \in I$ ossia se $AI \subset I$, dove $AI : \{ax \,|\, x \in I, a \in A\}$

Esempi:

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

  Verifica delle condizioni per l'ideale

  - Abbiamo già verificato nella sezione 2.1 che $(I(a), +) \subset (A, +)$
  - Sappiamo già che $a \in A$, dunque verifichiamo che:

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

- Siano $a_1, a_2 \in A$, dove A è un anello commutativo, e sia $I(a_1, a_2) : \{a_1b_1 + a_2b_2 \,|\, b_1, b_2 \in A\}$. Verifichiamo che $I(a_1, a_2) \subset A$ è ancora un ideale di A:

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

- Analogamente ai due casi precedenti, possiamo verificare che anche $I(a_1, ..., a_n)$ risulta essere un'ideale di A.

- Se $(A, +, \cdot)$ è un anello commutativo e $I \subset A$, allora in particolare abbiamo che $(I, +) \subset (A, +)$ induce la **relazione di congruenza modulo I** (come visto nella sezione 2.1.1):
$$x \sim y \implies y - x \in I \Longrightarrow x \equiv y (\text{mod } I)$$
Se le operazioni additiva e moltiplicativa sono ben definite, ossia si ha che $[x]+[y] = [x+y]$ e che $[x][y] = [xy]$, allora $(A/I, +, \cdot)$ è un **anello commutativo**.

  Dimostrazione:

  - Abbiamo già visto nella sezione 2.1.1 che $(A/I, +)$ sia un 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:
    * $x \equiv x' (\text{mod } I) \implies i_1 := x' - x \in I$
    * $y \equiv y' (\text{mod } I) \implies i_2 := y' - y \in I$
    * $xy \equiv x'y' (\text{mod } I) \implies x'y' - xy \in I$

    $$x'y' - xy = x'y' + xy' - xy' - xy = (x' - x)y' + x(y' - y) = i_1 y' + x i_2$$

    Siccome $i_1 y', x i_2 \in I$ ne segue che $x'y' - xy = i_1 y' + x i_2 \in I$, l'operazione prodotto è ben definita.

- Analogamente a quanto fatto per la somma, considerando l'anello commutativo $(\mathbb{Z}, +, \cdot)$ e il suo ideale principale $I(n)$, otteniamo che anche **il gruppo quoziente** $\mathbb{Z}_n = \mathbb{Z}/I(n)$ **sia un anello commutativo**.

  Ad esempio, in $\mathbb{Z}_4$ avremo che:

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

2.3 Invertibili e Divisori dello zero

Definition 13. Invertibili e Divisori dello zero

Dato un anello commutativo $(A, +, \cdot)$ e dato un elemento $a \in A$, affermiamo che tale elemento è un **invertibile** se $\exists a^{-1} \in A \,|\, aa^{-1} = a^{-1}a = 1$, mentre affermiamo che esso è un **divisore dello zero** se $a \,|\, 0 \implies \exists B \in A, 0 = ab$.

Denotiamo come $A^* \subset A$ l'**insieme di tutti gli invertibili di** A e affermiamo che A è un **dominio di integrità** se l'unico elemento divisore dello zero è lo zero stesso.

Observation 9

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 $\exists a, b \in A^*, b \neq 0 \,|\, 0 = ab, aa^{-1} = 1$. 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 10

A può essere un dominio di integrità se e solo se vale la **legge di annullamento del prodotto**, ossia

$$xy = 0 \implies x = 0 \vee y = 0$$

Observation 11

$(A^*, \cdot)$ è un gruppo, poiché:

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

Observation 12

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

Observation 13

$\mathbb{Z}_n$ è un dominio di integrità se e solo se n è un numero primo. In tal caso, inoltre, usiamo la notazione $\mathbb{Z}_p$ per dire che si tratta dell'insieme quoziente di un numero primo.

Dimostrazione:

- Supponiamo che n non sia primo, implicando che n possa essere espresso come il prodotto di due fattori ab:

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

- Tuttavia, in $\mathbb{Z}_n$ abbiamo che $[n] = [0]$, implicando che $[n] = [ab] = [0]$, andando in conflitto col fatto che $a, b > 0 \implies [a][b] \neq [0]$.
- Di conseguenza, si ha che $a \mid 0$ e $b \mid 0$, dunque $\mathbb{Z}_n$ non può essere un dominio di integrità.
- Supponiamo invece che solo $[a] \in \mathbb{Z}_n$ sia un divisore dello zero. In tal caso, si ha:

$$\exists 0 < b < n \in \mathbb{Z}_n \mid [a][b] = [0] = [ab] \implies n \mid ab \implies$$

$$\implies n \mid a \vee n \mid b \implies [a] = [n] = [0] \vee [b] = [n] = [0]$$

- Dunque, l'ipotesi $0 < b < n$ viene contraddetta, dunque è impossibile che esistano $a, b \neq 0 \in \mathbb{Z}_p$ tali che $a \mid 0$ e $b \mid 0$.

Lemma 4. Numeri primi e fattorizzazioni

Se $n \in \mathbb{N}$, allora $n \mid ab \implies n \mid a \vee n \mid b$

2.4 Massimo comun divisore

Definition 14. Massimo comun divisore (MCD)

Sia I un ideale di $\mathbb{Z}$, allora esiste un **unico intero** $d \geq 0$ tale che $I = I(d)$ dove $I(d) : \{ad \mid a \in \mathbb{Z}\}$.

Sia $a, b \in \mathbb{Z}$. Allora si ha che:

$$I(a, b) : \{ax + by \mid x, y \in \mathbb{Z}\} \implies \exists! d \geq 0 \mid I(a, b) = I(d)$$

dove denotiamo $d := MCD(a, b)$, ossia il **massimo comun divisore**.

In particolare, si ha che:

$$\exists x, y \in \mathbb{Z} \mid ax + by = d := MCD(a, b)$$

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 $I = I(d)$:

- $I(d) \subseteq I$:
  - $x \in I(d) \implies \exists y \in \mathbb{Z} \,|\, x = yd$
  - Per l'assioma degli ideali $IA \subset I$, 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 :

    $$\exists! q \in Z, 0 \leq r < d \,|\, x = dq + r$$

  - 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 $dq \in I(d) \implies dq \in I$

Alla luce di ciò, affermiamo che dati $a_1, ..., a_n \in \mathbb{Z}$, il loro $d := MCD(a_1, ..., a_n)$ è l'**unico intero** $d \geq 0 \,|\, I(d) = I(a_1, ..., a_n)$.

Observation 14

Dati due ideali principali $I(a)$ e $I(b)$ si verifica che $I(a) = I(b) \iff a = \pm b$

Dimostrazione:

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

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

$$\implies -x = -(ay) = a(-y) \in I(a) \implies -x = -(ay) = (-a)y \in I(-a)$$

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

$$I(a) = I(b) \implies a \in I(b), b \in I(a) \implies p, q \in \mathbb{Z} \,|\, a = bp, b = qa \implies$$
$$\implies a = (qa)a \implies pq = 1 \implies p = q = \pm 1$$

  Quindi gli unici due casi possibili sono $p = q = 1 \implies a = b$ e $p = q = -1 \implies a = -b$

Observation 15

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

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

Dimostrazione:

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

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

Proposition 5

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:

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

  Sia $d := MCD(a, n) > 0$. Dunque abbiamo che:

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

  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 1

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

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

Corollary 2

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 $[3]x + [2] = [0]$:

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

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

2.4.1 Calcolo del MCD

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

Esempi:

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

$$MCD(2^4 \cdot 3^3 \cdot 5 \cdot 7, 2^3 \cdot 3^3 \cdot 7^2 \cdot 11) = 2^3 \cdot 3^2 \cdot 7$$

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 $r_n \,|\, d$ e $d \,|\, r_n$.

- Verifichiamo che $d \,|\, r_n$:

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

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

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

  Di conseguenza, abbiamo che $d \,|\, r_n$

- Verifichiamo che $r_n \,|\, d$:

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

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

  $$r_n \,|\, r_n \wedge r_n \,|\, r_{n-1} \implies r_n \,|\, r_{n-2}$$
  $$r_n \,|\, r_{n-1} \wedge r_n \,|\, r_{n-2} \implies r_n \,|\, r_{n-3}$$
  $$...$$
  $$r_n \,|\, r_1 \wedge r_n \,|\, r_0 \implies r_n \,|\, d$$

  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:
$$x, y \in \mathbb{Z} \,|\, MCD(488, 216) = 216x + 448y$$
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 $x = -1, y = 12, z = -18$

2.4.2 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 6

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 $\exists k \in \mathbb{Z} \mid N = mk$:

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

2.4.3 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:

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

Quindi:

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

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

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

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

Esempi:

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

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

  Tuttavia, siccome $3 \not| 40$, ne segue che $3 \not| 129383716$
- Vogliamo sapere se $3 \mid 129383716$. Siccome siamo in $\mathbb{Z}_{11}$ abbiamo che:

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

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

2.5 Operazioni sugli ideali

Dato un anello commutativo A e due ideali $I, J \subset A$, definiamo le seguenti operazioni binarie su di essi:

- **Somma tra ideali**:
  $$I + J : \{i + j \mid i \in I, j \in J\}$$
  Se $I, J \subset A$ sono ideali di A, allora anche $I + J \subset A$ è ideale

  Dimostrazione:

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

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

- **Intersezione tra ideali**:

$$I \cap J : \{i \,|\, i \in I \wedge i \in J\}$$

Se $I, J \subset A$ sono ideali di A, allora anche $I \cap J \subset A$ è ideale.

Dimostrazione:

– $I \cap J$ è sottogruppo di A, poiché:

  * $0 \in I \wedge 0 \in J \implies 0 \in I \cap J$
  * $x, y \in I \cap J \implies x, y \in I \wedge x, y \in J \implies x + y \in I \wedge x + y \in J \implies x + y \in I \cap J$
  * $x \in I \wedge x \in J \implies -x \in I \wedge -x \in J \implies -x \in I \cap J$

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

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

- **Prodotto tra ideali**:

$$I \cdot J : \{i_1 j_1 + i_2 j_2 + ... + i_n j_n \,|i_1, i_2 ..., i_n \in I, j_1, j_2 ..., j_n \in J\}$$

Se $I, J \subset A$ sono ideali di A, allora anche $I \cdot J \subset A$ è ideale.

Dimostrazione:

– $I \cap J$ è sottogruppo di A, poiché:

  * $0 \in I \wedge 0 \in J \implies 0 = 0 + 0 \in I \cdot J$
  * $x = i_1 j_1 + i_2 j_2 + ... + i_n j_n \in I \cdot J$

    $y = i'_1 j'_1 + i'_2 j'_2 + ... + i'_n j'_n \in I \cdot J$

    $\implies x + y = i_1 j_1 + i'_1 j'_1 + ... + i_n j_n + i'_n j'_n \in I \cdot J$
  * $x \in I \cdot J \implies -x = x = (-i_1) j_1 + (-i_2) j_2 + ... + (-i_n) j_n \,|\, -i_k \in I \implies -x \in I \cdot J$

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

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

$$\implies ax \in I \cdot J$$

2.5.1 Caso particolare in $\mathbb{Z}$

Ricordando che **in $\mathbb{Z}$ ogni ideale è principale**, i due ideali I e J appaiono nella forma $I(a)$ e $I(b)$. Da ciò nascono una serie di implicazioni riguardanti le tre operazioni sopra descritte:

- $I + J = I(a) + I(b) = I(d)$ 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. (*Dimostrazione a seguire nella sezione successiva*)

2.6 Minimo comune multiplo

Definition 15. 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 $a_1, ..., a_n$:

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

2.6.1 Calcolo del mcm e 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 7. 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 $a = 0 \lor b = 0$, 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 $p \not| n \implies n_p = 0$

- 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:

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

2.7 Teorema cinese dei resti

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

Lemma 8. 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

$$MCD(a_i, a_j) = 1, \forall i \neq j \implies \forall p \in \mathbb{P}, p \,|\, a_i \implies p \not| a_j, \forall j \neq i$$

- 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 9. 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:

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

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

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

Theorem 10. 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**

$$\begin{cases} x \equiv b_1 (\bmod\ a_1) \\ x \equiv b_2 (\bmod\ a_2) \\ ... \\ x \equiv b_3 (\bmod\ a_n) \end{cases}$$

ammette un'unica soluzione $x \bmod q$ 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 $\exists x \bmod \mathtt{m} \in \mathbb{Z}_m$, abbiamo che

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

  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 $x \equiv 23 \pmod{105}$ è l'unica soluzione del sistema. Difatti, verifichiamo che:

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

2. - Cerchiamo una soluzione per il seguente sistema:

$$\begin{cases} x \equiv 6 \pmod{15} \\ x \equiv 9 \pmod{20} \end{cases}$$

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

$$x \equiv 6 \pmod{15} \implies \begin{cases} x \equiv 0 \pmod{3} \\ x \equiv 1 \pmod{5} \end{cases}$$

$$x \equiv 9 \pmod{20} \implies \begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 4 \pmod{5} \end{cases}$$

- Il nuovo sistema sarà quindi:

$$\begin{cases} x \equiv 6 \pmod{15} \\ x \equiv 9 \pmod{20} \end{cases} \implies \begin{cases} x \equiv 0 \pmod{3} \\ x \equiv 1 \pmod{5} \\ x \equiv 1 \pmod{4} \\ x \equiv 4 \pmod{5} \end{cases}$$

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

3. - Cerchiamo una soluzione per il seguente sistema:

$$\begin{cases} x \equiv 6 \pmod{15} \\ x \equiv 11 \pmod{20} \\ x \equiv 15 \pmod{21} \end{cases}$$

- Scomponendo in fattori primi si ha che:

$$x \equiv 6 \pmod{15} \implies \begin{cases} x \equiv 0 \pmod{3} \\ x \equiv 1 \pmod{5} \end{cases}$$

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

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

- Il nuovo sistema sarà quindi:

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

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

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

- Dunque $[a] = [2] \implies a \equiv 2(\text{mod } 5) \implies a = 2 + 5b, \forall b \in \mathbb{Z}$.
- Sostituendo nella terza congruenza otteniamo $x = 3(2 + 5b) = 6 + 15b \implies 6 + 15b \equiv 3(\text{mod } 4)$. 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 $[b] = [3] \implies b \equiv 3(\text{mod } 4) \implies b = 3 + 4c, \forall c \in \mathbb{Z}$
- Sostituendo nella quarta congruenza otteniamo $x = 6 + 15(3 + 4c) = 51 + 60c \implies 51 + 60c \equiv 1(\text{mod } 7)$. 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 $[c] = [2] \implies c \equiv 5(\texttt{mod}\ 7) \implies c = 5 + 7d, \forall d \in \mathbb{Z}$.
- Infine, otteniamo che

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$[1] + [48][j] = [2]$$

$$[j] = [1][3]^{-1}$$

$$[j] = [2]$$

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

2.8 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 16. 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:

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

L'induzione matematica sarà alla base di alcune dimostrazioni che vedremo in seguito, come il **piccolo teorema di Fermat** mostrato nella sezione successiva.

2.9 Piccolo teorema di Fermat

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

Lemma 11

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

$$p \,\Big|\, \binom{p}{k}$$

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:

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

  Esempio:

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

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 $p \,|\, n$, in $\mathbb{Z}_p$ si ha:

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

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

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

Lemma 12

In $\mathbb{Z}_p$ si ha che:

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

Dimostrazione:

- Dato il binomio di Newton, 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:
$$([a_1] + ... + [a_n] + [a_{n+1}])^p = ([[a_1] + ... + [a_n]] + [a_{n+1}])^p = ([a_1] + ... + [a_n])^p + [a_{n+1}]^p =$$
$$= ([a_1] + ... + [a_{n-1}])^p + [a_n]^p + [a_{n+1}]^p = ... = [a_1]^p + ... + [a_{n+1}]^p$$

Theorem 13. 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 $a^{p-3} \equiv a^{-2} (\texttt{mod}\ \ p)$ e che $5^7 \equiv 5^5 \equiv 5^3 \equiv 5 \equiv 2 (\texttt{mod}\ \ 3)$.

2.10 Ordine di un elemento di un gruppo

Consideriamo un gruppo G non per forza abeliano e sia $g \in G$. Definiamo il sottogruppo $H(g) \subset G$ e l'ideale $I(g) \subset \mathbb{Z}$ come:

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

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

dove e è l'elemento neutro della moltiplicazione e g^n è definita come:

$$g^n = \begin{cases} \prod_{i=0}^{n} g & \text{se } n > 0 \\ e & \text{se } n = 0 \\ \prod_{i=0}^{n} g^{-1} & \text{se } n < 0 \end{cases}$$

Prima di tutto, dimostriamo che essi siano rispettivamente un sottogruppo di G ed un ideale di $\mathbb{Z}$:

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

A questo punto, diamo una definizione di ordine di un elemento di un gruppo:

Definition 17. Ordine di un elemento di un gruppo

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

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

Affermiamo, inoltre, la seguente proposizione:

Proposition 14

Dato $g \in G$ e dato $I(g) : \{n \in \mathbb{Z} \,|\, g^n = e\}$, allora $\exists! d \geq 0 \,|\, I(g) = I(d)$ dove:

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

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 $n \in \mathbb{Z}$ tale che:

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

    concludendo che $H(g)$ possa contenere al massimo d elementi, dunque $o(g) := |H(g)| \leq d$
  - Mostriamo ora che poiché $0 \leq m, n < d \implies -d < m, n < d$ e poiché $g^n = g^m \implies d \mid m - n$, l'unico numero $m - n$ in grado di soddisfare entrambe le condizioni è l'unico multiplo di d compreso tra $-d$ e d, ossia 0
  - Dunque, si ha che $m - n = 0 \implies m = n$, implicando quindi che

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

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

Proposition 15

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

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

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

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

Dimostrazione:

- Dato $d := o(g)$, 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 $[a]^p = [0]$
- Per $[a] \neq [0]$, ricordiamo che $\mathbb{Z}_p$, dove $p \in \mathbb{P}$, corrisponde ad un campo, dunque tutti i suoi elementi, tranne lo zero, sono invertibili. 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 $[a] \in \mathbb{Z}_{|}^*$ si ha che:
$$[a]^{\left|\mathbb{Z}_p^*\right|} = [1] \implies [a]^{p-1} = [1] \implies [a]^p = [a]$$

2.10.1 Ordine di una permutazione

Un caso particolare di ordine di un elemento appartenente ad un gruppo è quello delle **permutazioni** (si consiglia di rivedere la sezione 1.2.1)

Dato $\sigma \in S_n$, definiamo come **ciclo di** σ una sequenza di interi $1 \leq i_1, ..., i_n \leq n$ tutti distinti tra loro tali che:

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

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:

- $1 \to 5 \to 2 \to 7 \to 1$
- $3 \to 6 \to 3$
- $4 \to 9 \to 8 \to 4$

Definiamo come **lunghezza di un ciclo** il numero di elementi appartenenti a tale ciclo. Nel nostro esempio, quindi, abbiamo tre cicli di lunghezza rispettiva 4, 2 e 3. In particolare, utilizziamo la seguente notazione per descrivere la **decomposizione in cicli** della permutazione:

$$\sigma = (1587)(36)(498)$$

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

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

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

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

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

dove `id` rappresenta la **permutazione identica**, ossia quella che manda ogni elemento in se stesso. 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 $\sigma \in S_n$ dove $\sigma(i) = i$, dunque i viene sempre mandato in se stesso, allora $\sigma^k(i) = i, \forall k \in \mathbb{Z}$.

Lemma 16

Se $i \leq i \leq n$ è un elemento appartenente ad un ciclo di σ di lunghezza d, allora

$$I(\sigma, i) = I(d)$$

Dimostrazione:

- Per dimostrare il lemma, 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:
  - $\sigma(i_1) = i_2 \neq i_1$
  - $\sigma^2(i_1) = \sigma(\sigma(i_1)) = \sigma(i_2) = i_3 \neq i_1$
  - ...
- Più in generale, quindi, affermiamo 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:

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

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

Lemma 17. Ordine di una permutazione

Dato $\sigma \in S_n$ 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:

- Dato $\sigma \in S_7$ 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:

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

- Dato $\sigma \in S_{15}$ 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:

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

2.11 Segno delle permutazioni

Dato $\sigma \in S_n$, 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:

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

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 18. Segno di una permutazione

Dato $\sigma \in S_n$ e dato l'insieme delle sue inversioni definito come

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

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.

Dati $1 \leq i < j \leq n$, definiamo come **trasposizione** un particolare tipo di permutazione $\tau_{i,j} \in S_n$ 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 18

Data una permutazione $\sigma \in S_n$, essa può essere espressa come il **prodotto di** k **trasposizioni adiacenti**:

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

Dimostrazione tramite esempio:

- Osserviamo prima come dati $\sigma, \tau_{i,j} \in S_n$, quindi definiti come:

$$\sigma = \begin{pmatrix} 1 & ... & i & ... & j & ... & n \\ \sigma(1) & ... & \sigma(i) & ... & \sigma(j) & ... & \sigma(n) \end{pmatrix}$$

$$\tau_{i,j} = \begin{pmatrix} 1 & ... & i & ... & j & ... & n \\ 1 & ... & j & ... & i & ... & n \end{pmatrix}$$

  si ha che:

$$\sigma\tau_{i,j} = \begin{pmatrix} 1 & ... & i & ... & j & ... & n \\ \sigma(1) & ... & \sigma(j) & ... & \sigma(i) & ... & \sigma(n) \end{pmatrix}$$

- Ad esempio, quindi, dato $\sigma \in S_3$ definito come:

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

  abbiamo che:

$$\sigma \cdot \tau_{3,4} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \implies \sigma \cdot \tau_{3,4} \cdot \tau_{2,3} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \implies$$

$$\implies \sigma{\cdot}\tau_{3,4}{\cdot}\tau_{2,3}{\cdot}\tau_{1,2} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \implies \sigma{\cdot}\tau_{3,4}{\cdot}\tau_{2,3}{\cdot}\tau_{1,2}{\cdot}\tau_{3,4} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \texttt{id}$$

- Dunque, si ha che:

$$\sigma(\tau_{3,4}\tau_{2,3}\tau_{1,2}\tau_{3,4}) = \texttt{id}$$
$$\sigma(\tau_{3,4}\tau_{2,3}\tau_{1,2}\tau_{3,4})(\tau_{3,4}\tau_{2,3}\tau_{1,2}\tau_{3,4})^{-1} = \texttt{id}(\tau_{3,4}\tau_{2,3}\tau_{1,2}\tau_{3,4})^{-1}$$
$$\sigma = (\tau_{3,4}\tau_{2,3}\tau_{1,2}\tau_{3,4})^{-1}$$
$$\sigma = \tau_{3,4}\tau_{1,2}\tau_{2,3}\tau_{3,4}$$

Proposition 19

Dato $\sigma \in S_n$ dove $\sigma = \tau_1 \cdot ... \cdot \tau_k$ dove $\tau_i = \tau_{i,i+1} \in S_n$ (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:

$$\sigma\tau = \begin{pmatrix} 1 & ... & i & i+1 & ... & n \\ \sigma(1) & ... & \sigma(i+1) & \sigma(i) & ... & \sigma(n) \end{pmatrix}$$

- 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:

$$sgn(\sigma\tau) = -sgn(\sigma)$$

- Dato $\sigma = \tau_i \cdot ... \cdot \tau_k$, si ha che:

$$\sigma(\tau_i \cdot ... \cdot \tau_k)^{-1} = (\tau_i \cdot ... \cdot \tau_k)(\tau_i \cdot ... \cdot \tau_k)^{-1} = \mathtt{id}$$

- Poiché `id` non ha alcuna inversione per sua definizione stessa, si ha che $sgn(\mathtt{id}) = 1$. Di conseguenza, si verifica che:

$$1 = sgn(\mathtt{id}) = sgn(\sigma(\tau_i \cdot \tau_2 \cdot \tau_3 \cdot ... \cdot \tau_k)^{-1}) = sgn(\sigma \cdot \tau_k \cdot ... \cdot \tau_3 \cdot \tau_2 \cdot \tau_1) =$$

$$= -sgn(\sigma \cdot \tau_k \cdot ... \cdot \tau_3 \cdot \tau_2) = sgn(\sigma \cdot \tau_k \cdot ... \cdot \tau_3) = ... = (-1)^k \cdot sgn(\sigma)$$

- Quindi, affermiamo che:

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

Corollary 3

Date due permutazioni $\sigma, \sigma' \in S_n$, si verifica che:

$$sgn(\sigma\sigma') = sgn(\sigma) \cdot sgn(\sigma')$$

Dimostrazione:

- Dato $\sigma = \tau_1 \cdot ... \cdot \tau_k$ 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 4

Data una permutazione $\sigma \in S_n$,si verifica che:

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

Dimostrazione:

- Poiché
$$1 = sgn(\texttt{id}) = sgn(\sigma\sigma^{-1}) = sgn(\sigma) \cdot sgn(\sigma^{-1})$$
allora si ha che:
$$1 = sgn(\sigma) \cdot sgn(\sigma^{-1}) \implies sgn(\sigma) = sgn(\sigma^{-1})$$

Corollary 5

Denotiamo il sottogruppo $A_n \subset S_n$ come **gruppo alterno di ordine** n, definito come:

$$A_n := \{\sigma \in S_n \,|\, sgn(\sigma) = +1\}$$

Inoltre, abbiamo che σ e σ' sono nella stessa classe laterale 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 S_n venga diviso dal sottogruppo A_n in esattamente due partizioni, una contente tutte le permutazioni pari ed una contenente tutte le dispari.

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

$$2 = |S_n/A_n| = \frac{|S_n|}{|A_n|} \implies |A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$$

Vogliamo ora dimostrare che data $\sigma \in S_n$ e data la sua scomposizione in cicli $\sigma = \gamma_1 ... \gamma_k$, si ha che $sgn(\sigma) = (-1)^{n-k}$.

Prima di ciò, è necessario introdurre la **relazione di coniugato**.

Definition 19. Relazione di coniugato

Dato un gruppo G e dati $g, h \in G$, diciamo che g è coniugato di h (denotato come $g \sim h$) se si verifica che:

$$\exists a \in G \,|\, h = aga^{-1}$$

Observation 16

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

$$h = aga^{-1} = aa^{-1}g = g$$

Observation 17

La relazione di coniugato è una relazione di equivalenza.

Dimostrazione:

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

- **Simmetria**:
$$g \sim h \implies h = aga^{-1} \implies a^{-1}ha = a^{-1}aga^{-1}a \implies a^{-1}ha = g$$
ponendo $b := a^{-1}$, si ha che:
$$bhb^{-a} = g \implies h \sim g$$

- **Transitività**:
$$g \sim h \wedge h \sim k \implies h = aga^{-1}, k = bhb^{-1} \implies k = b(aga^{-1})b^{-1} = (ba)g(a^{-1}b^{-1})$$
ponendo $c := ba$, si ha che:
$$k = cgc^{-1} \implies g \sim k$$

In particolare, nel **caso delle permutazioni**, dati $\sigma, \sigma' \in S_n$ si ha che:

$$\exists \alpha \in S_n \,|\, \sigma = \alpha\sigma\alpha^{-1} \implies sgn(\sigma') = sgn(\alpha) \cdot sgn(\sigma) \cdot sgn(\alpha^{-1})$$

Tuttavia, poiché $sgn(\alpha) = sgn(\alpha^{-1}) = \pm 1 \implies sgn(\alpha) \cdot sgn(\alpha^{-1}) = 1$, si ha che:

$$sgn(\sigma') = sgn(\alpha) \cdot sgn(\sigma) \cdot sgn(\alpha^{-1}) = sgn(\sigma)$$

Proposition 20

Dati $\sigma, \sigma' \in S_n$, 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:

$$\sigma \sim \sigma' \iff \begin{cases} k = h \\ d_1 = d'_1 \\ d_2 = d'_2 \\ ... \\ d_k = d'_h \end{cases}$$

Dimostrazione:

- Supponiamo che $\sigma \sim \sigma'$, dunque $\exists \alpha \in S_n \mid \sigma' = \alpha\sigma\alpha^{-1}$
- 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 $\alpha \in S_n \mid \alpha(i_k) = a_k, ..., \alpha(j_h) = b_h$
- 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 21

Dato $\sigma \in S_n$ e data la sua scomposizione in cicli $\sigma = \gamma_1 ... \gamma_k$, allora si ha che:

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

Dimostrazione:

- Supponiamo che $\exists \sigma' \in S_n \,|\, \sigma' \sim \sigma$. 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:

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

2.12 Morfismi

Definition 20

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 18

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 19

Se $f : G \to H$ è un **morfismo biettivo** (dunque sia un morfismo, sia una funzione biettiva), 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 21. 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 1.3.2, 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 $(H, \cdot) \subset (\mathbb{C}^*, \cdot)$ 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 2.10, siccome $o(g) < +\infty$, allora $g^n = 1_G = g^0$ per qualche $n > 0$, implicando che $\exists n \neq 0 \,|\, g^n = g^0$, 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:

$$\exists n \neq m \,|\, g^n = g^m \implies g^0 = 1_G = g^{-n} \cdot g^n = g^{-n} \cdot g^m = g^{m-n} \implies$$
$$\implies \exists m - n \neq 0 \,|\, g^{m-n} = 1_G$$

     Come visto nella sezione 2.10, poiché $I(g) = I(d)$ e poiché $d > 0$ (dato che $\exists m-n \neq 0 \,|\, g^{m-n} = 1_G$, 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 $f : (\mathbb{Z}_m, +, \cdot) \to (\mathbb{Z}_{\ltimes}, +, \cdot) :$ `x mod m` $\to$ `x mod n` è un morfismo se e solo se $n \,|\, m$:

$$\texttt{x mod m} + \texttt{y mod m} = \texttt{(x+y) mod m} = \texttt{(x+y) mod n}$$
$$\texttt{x mod m} \cdot \texttt{y mod m} = \texttt{(xy) mod m} = \texttt{(xy) mod n}$$

   Attenzione: l'ultimo passaggio di entrambe le equazioni è possibile se e solo se $n \,|\, m$.

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:

$$F_g(h)F_g(h') = (ghg^{-1})(gh'g^{-1}) = ghh'g^{-1} = F_g(hh')$$

2.12.1 Nucleo ed Immagine di un morfismo

Proposition 22. 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 $Ker(f) \subset G$, detto **nucleo di** f, e un sottogruppo $Im(f) \subset H$, detto **immagine di** f, dove:

$$Ker(f) : \{g \in G \,|\, f(g) = 1_H\}$$

$$Im(f) : \{y \in H \,|\, f(x) = y, \exists x \in G\}$$

Dimostrazione:

- $Ker(f) \subset G$:
  - $f(1_G) = 1_H \implies 1_G \in Ker(f)$
  - $x, y \in Ker(f) \implies f(x) = f(y) = 1_H \implies f(xy) = f(x)f(y) = 1_H \cdot 1_H = 1_H \implies xy \in Ker(f)$
  - $x \in Ker(f) \implies f(x) = 1_H \implies 1_H = 1_H^{-1} = f(x)^{-1} = f(x^{-1}) \implies x^{-1} \in Ker(f)$
- $Im(f) \subset H$:
  - $f(1_G) = 1_H \implies 1_G \in Im(f)$
  - $x, y \in Im(f) \implies x = f(g), y = f(h) \implies xy = f(g)f(h) = f(gh) \implies xy \in Im(f)$
  - $x \in Im(f) \implies x = f(g) \implies x^{-1} = f(g)^{-1} = f(g^{-1}) \implies x^{-1} \in Im(f)$

Observation 20

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 21

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

$$Ker(f) : \{a \in A \,|\, f(a) = 0_B\}$$

$$Im(f) : \{b \in B \,|\, f(a) = b, \exists a \in A\}$$

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 $(B, +)$

2.13 Teorema fondamentale di isomorfismo

Definiamo ora una **struttura algebrica intermedia tra sottogruppo ed ideale**, detta sottoanello:

Definition 22. Sottoanello

Dato un anello A definiamo $(B, +, \cdot) \subset (A, +, \cdot)$ come sottoanello se:

- $(B, +) \subset (A, +)$ è sottogruppo
- $x, y \in B \implies x \cdot y \in B$ (dunque chiusa nella seconda operazione)

Observation 22

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 23. 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:
$$[a], [b] \in A/Ker(f) \,|\, [a] = [b] \implies f(a) = f(b)$$
è vero poichè:
$$[a] = [b] \iff a \equiv b(\texttt{mod}\ Ker(f)) \iff b - a \in Ker(f) \iff$$
$$\iff 0_B = f(b-a) = f(b) - f(a) \iff f(a) = f(b)$$
- 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:
$$[x] \in A/Ker(f) \,|\, \varphi([x]) = 0_A \iff f(x) = 0_A \iff x \in Ker(f) \iff [x] = [0_A]$$
- 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:

$$\zeta^k = 1 \iff n \,|\, k \implies Ker(f) = I(n)$$

Dimostrazione:

- Vediamo che $I(n) \subseteq Ker(f)$
$$n \,|\, k \implies k = np \in I(n) \implies \zeta^k = \zeta^{np} = (\zeta^n)^p = 1_H^p = 1_H \in Ker(f)$$

- 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 6

Dato il morfismo $f : (\mathbb{Z}, +, \cdot) \to (\mathbb{C}^*, +, \cdot) : k \mapsto \zeta^k$, per il teorema fondamentale di isomorfismo si ha che:

$$H(\zeta) = Im(f) \cong \mathbb{Z}/Ker(f) = \mathbb{Z}/I(n) = \mathbb{Z}_n$$

2.14 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 23

Se A è un anello e $B \subset A$ 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 23. Classi laterali sinistre e destre

Sia $(G, \cdot)$ un gruppo e sia $H \subset G$ sottogruppo. Possiamo definire due relazioni di equivalenza del tipo:

$$x \sim_S y \iff x^{-1}y \in H \qquad\qquad x \sim_D y \iff xy^{-1} \in H$$

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).

$$[x]_S : \{y \in G \,|\, x \sim_S y\} \qquad\qquad [x]_D : \{y \in G \,|\, x \sim_D y\}$$

Observation 24

Come visto nella sezione 2.1.1, si ha che:

$$[x]_S = xH = \{xh \,|\, h \in H\} \qquad\qquad [x]_D = Hx = \{hx \,|\, h \in H\}$$

Observation 25

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 26

Se il sottogruppo non è commutativo, non è detto che $xH = Hx, \forall x \in G$ (si pensi ad esempio alle permutazioni)

A questo punto, diamo una definizione di **sottogruppo normale**:

Definition 24. Sottogruppo normale

Sia $(G, \cdot)$ un gruppo e sia $H \subset G$ 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 24

Dato $(G, \cdot)$ gruppo e $H \subset G$ sottogruppo, le seguenti condizioni sono **equivalenti tra loro**:

1. H è un sottogruppo normale
2. $\forall g \in G, h \in G \implies ghg^{-1} \in H$
3. $g \in G, h \in G \implies \exists k \in H \,|\, gh = kg$

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)
$$gh \in gH = Hg = \{kg \,|\, k \in H\} \implies gh = kg$$
- 3) $\implies$ 2)
$$g \in G, h \in H \implies \exists k \in H \,|\, gh = kg \implies ghg^{-1} = kgg^{-1} \implies ghg^{-1} = k \in H$$
- 2) $\implies$ 1)
  - Prendiamo $gh \in gH$ e definiamo $ghg^{-1} =: k \in H$
  - Allora si ha che
  $$ghg^{-1} = k \implies ghg^{-1}g = kg \implies gh = kg \implies kg \in Hg \implies gH \subset Hg$$
  - Prendiamo $xg \in Hg$ e definiamo $g^{-1}xg =: j \in H$
  - Allora si ha che
  $$g^{-1}xg = j \implies gg^{-1}xh = gj \implies gj \in gH \implies Hg \subset gH$$
  - Siccome $gH = Hg$, allora H è normale

Observation 27

La condizione 2) è equivalente a richiedere che H sia l'unione di tutte le classi di equivalenza della relazione di coniugio

Observation 28

Un sottogruppo di un gruppo abeliano è sempre normale, poiché la condizione $xH = Hx$ viene soddisfatta dalla proprietà commutativa

Proposition 25

Se $(G, \cdot)$ è un gruppo e $H \subset G$ 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 7

Se $f : G \to H$ è un morfismo di gruppi, allora $Ker(f) \subset G$ è sottogruppo normale e $Im(f) \subset H$ è sottogruppo

Dimostrazione:

- Sappiamo già che $Ker(f) \subset G$ e che $Im(f) \subset H$ 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 26. 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 2.13)

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:

$$Ker(f) = H(g) = \{g^n \,|\, n \in \mathbb{Z}\}$$

$$Im(f) = I(g) = \{n \in \mathbb{Z} \,|\, g^n = 1_G\}$$

- 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 8

Se G è un gruppo finito dove $|G| = n, p \in \mathbb{P}$, 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

$$G = H \cong \mathbb{Z}_p$$

Observation 29

Se $H \subset G$ 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:

$$f(xy) = [xy] = [x][y] = f(x)f(y)$$

- $Ker(f) = H$:

$$g \in Ker(f) \iff f(g) = [g] = [1_G] = 1_g \cdot H = H \iff g \in H$$