Algebra 1 - Moci

Algebra di Base

Definizione di Insieme: Un Insieme è definito come una collezione di elementi (di qualsiasi genere)

$x \in A$: si legge "x è un elemento dell'insieme A"
$x \notin A$ si legge "x non è un elemento che fa parte dell'insieme A"
$A \subseteq B$ si legge "L'insieme A è contenuto o uguale all'insieme B"
$B \subseteq A$ si legge "L'insieme B è contenuto o uguale all'insieme A"

Da queste ultime due affermazioni si può dedurre che $A = B$, ossia che "l'insieme A è uguale all'insieme B" o che "tutti gli elementi contenuti in A sono anche contenuti in B"

Definizione di Insieme delle Parti: Dato un insieme A, si può definire Insieme delle Parti $\mathcal{P}(A)$ quell'insieme che contiene tutti i sottoinsiemi di A.

Esempio:
Dato l'insieme $A = \{x; y; z\}$, allora l'insieme $\mathcal{P}(A) = \{\varnothing; \{x\}; \{y\}; \{z\}; \{x; y\}; \{x; z\}; \{y; z\}; \{x; y; z\}\}$
È possibile inoltre poter indovinare di quale sottoinsieme si sta trattando con tre semplici domande:
- "Contiene x?"
- "Contiene y?"
- "Contiene z?"

Operazioni binarie (ossia da due elementi ne ottengo uno soltanto):

- Unione $A \cup B \Leftrightarrow B \cup A = \{x | x \in A \vee x \in B\}$
- Intersezione $A \cap B \Leftrightarrow B \cap A = \{x | x \in A \wedge x \in B\}$
  Su queste due operazioni sono valide sia la proprietà Commutativa sia quella Associativa
- Differenza Insiemistica $A \setminus B = \{x | x \in A \wedge x \notin B\}$
  Su quest'operazione non si posso applicare né la proprietà Commutativa né quella Associativa
- Prodotto Cartesiano: si definisce il Prodotto Cartesiano l'insieme $A \times B : \{(a; b), a \in A, b \in B\}$

Esempio:
$A = \{1; 2; 3; 4\} \quad B = \{x; y; z\}$
$A \times B = \{(1; x); (1, y); (1; z); (2; x); (2; y); \ldots; (4; z)\}$

Si osserva che se l'insieme A ha n elementi e l'insieme B ha m elementi, allora l'insieme $A \times B$ avrà $n \cdot m$ elementi

Si chiama apposta prodotto cartesiano perché (in caso si tratta di numeri) è possibile rappresentarlo in un grafico, nel quale il primo numero rappresenta l'asse delle ascisse, mentre il secondo numero quelle delle ordinate.

Definizione di Relazione: Una Relazione è un sottoinsieme R del prodotto cartesiano $A \times B$. Si dice che "a è in relazione con b se $(a; b) \in R$

Esempio:
Dati gli insiemi $A = B$ gli insiemi di tutte le rette, si può definire R l'insieme di tutte le rette con un punto in comune

Esistono vari tipi di Relazioni. Tra queste vi sono:

Relazione di Equivalenza: Si definisce Relazione di Equivalenza una relazione $R \subseteq A \times A$ che gode delle seguenti proprietà:

- Riflessiva (R): $(a; a) \in R \wedge a \in A$ ogni elemento è in relazione con sé stesso;
- Simmetrica (S): se $(a; b) \in R$, allora $(b; a) \in R \wedge a, b \in A$;
- Transitiva (T): se $(a; b) \in R$ e $(b; c) \in R$, allora $(a; c) \in R \wedge a, b, c \in A$.

Esempio:
Dato un Insieme A di numeri uguali:

(R) Un numero a è sempre uguale ad un numero a
(S) Se un numero a è uguale ad un numero b, allora il numero b è uguale al numero a (è sempre lo stesso numero)
(T) Se un numero a è uguale ad un numero b, e un numero b è uguale ad un numero c, allora il numero a è uguale al numero c

Relazione di Ordine: Si definisce una Relazione d'Ordine una relazione $R \subseteq A \times A$ che gode delle seguenti proprietà:

- Riflessiva (R): $(a; a) \subseteq R \wedge a \in A$ ogni elemento è in relazione con sé stesso;
- Antisimmetrica (A): se $(a; b) \in R$ e $(b; a) \in R$, allora $b = a$;
  se invertendo i valori a e b si ottiene lo stesso risultato allora $a = b$
- Transitiva (T): se $(a; b) \in R$ e $(b; c) \in R$, allora $(a; c) \in R \wedge a, b, c \in A$;

Esempio:
Dato un insieme di numeri $\mathbb{Z}$ si ha che $(a; b) \in R$ se $a \leq b$

Si definisce una Relazione d'Ordine Totale in $\mathbb{Z}$ se tutti gli elementi sono confrontabili attraverso il segno $\leq$, in particolare se dati qualunque a, b si ha che $(a, b) \in R$ oppure $(b, a) \in R$. In caso contrario viene definito Parziale.

L'Obiettivo di una Relazione di Equivalenza è quello di trovare degli aspetti di similitudine tra i vari elementi dell'insieme.
L'Obiettivo di una Relazione d'Ordine è quello di gerarchizzare gli elementi secondo una condizione.

È possibile rappresentare le Relazioni d'Ordine attraverso il diagramma di Hasse:

Un particolare tipo di Relazione d'Ordine si ha quando:
Dati $n \in \mathbb{N}$, $n > 1$ e dati $a, b \in \mathbb{Z}$ diciamo che $a \equiv b(n)$ se $n | a - b$, ossia "a è congruo a b in modulo n se n divide a-b "

Esempio:
$-7 \equiv 3 \equiv 18 \quad (5)$
$5 | 3 - 18 = 5 | 15 \quad 5 | 3 - (-7) = 5 | 10$

Osservazioni: Si può dire che un numero a è congruo ad un numero b se hanno lo stesso resto nella divisione per n. In particolare, se n è uguale a 2 e il resto è uguale a 0 il numero è pari, mentre se il resto è 1 allora è dispari.

Questa Relazione d'Ordine diventa una Relazione di Equivalenza quando $n \in \mathbb{Z}$:
Dimostrazione
(R) $a \in \mathbb{Z}, \quad a \equiv a \quad (n) \Rightarrow a - a = 0 \quad n | 0 = 0$
Visto che la differenza di un numero per sé stesso è 0, si ha che $\exists d : n \cdot d = a - a \Rightarrow n \cdot d = 0 d = 0$
(S) $a \equiv b \quad (n) \Rightarrow n | a - b \Leftrightarrow n | b - a \Rightarrow b \equiv a \quad (n)$
Questo perché $\exists d : d \cdot n = a - b \Rightarrow -d \cdot n = b - a$
Questo è il passaggio che rende la relazione d'Ordine (con $n \in \mathbb{N}$) una Relazione di Equivalenza (con $n \in \mathbb{Z}$)
(T) $a \equiv b \quad (n) \wedge b \equiv c \quad (n) \Rightarrow n | a - b \wedge n | b - c \Rightarrow n | (a - b) + (b - c) \Rightarrow n | a - c \Rightarrow a \equiv c \quad (n)$

Definizione di Classe di Equivalenza: Data una qualsiasi relazione di equivalenza (di uguaglianza o di congruenza) R di A (per cui si ha $R \subseteq A \times A$ per cui sono verificate le tre proprietà) invece di scrivere $(a, b) \in R$ si può scrivere $a \sim b$, in quanto sono accumulati da una relazione di equivalenza.
A questo punto per ogni $a \in A$ di può definire una classe di equivalenza tale che

$$[a] = \{x \in A \mid x \ \sim a\}$$

Esempio:
Siano $a, b \in A$, allora $[a] = [b] \Leftrightarrow a \sim b$
Per verificare la proposizione bisogna dimostrare entrambe le proposizioni:
$\Rightarrow$) Si ha che $[a] = [b] \Rightarrow a \sim b$
$\forall x \in A, x \in [b]$ (per p. Riflessiva) $a \in [b] \Rightarrow a \sim b$
$\Leftarrow$) Si ha che $a \sim b \Rightarrow [a] = [b]$
- Dimostriamo che $[a] \subseteq [b]$
Sia $x \in [a] \Rightarrow x \sim a$ (per Ipotesi si ha che $a \sim b$), per p. Transitiva $x \sim b \Rightarrow x \in [b]$
- Dimostriamo che $[b] \subseteq [a]$
Sia $x \in [b] \Rightarrow x \sim b$, per ipotesi si ha che $a \sim b$, per la proprietà Simmetrica si ha $x \sim b \wedge b \sim a$ per la proprietà

Transitiva $x \sim a \Rightarrow x \in [a]$
Avendo contemporaneamente $x \in [a]$ e $x \in [b]$ si giunge alla conclusione che $[a] = [b]$

Definizione di Insieme Quoziente: Si può definire l'insieme quoziente come l'insieme i cui elementi sono le classi di equivalenza

$$A_{/\sim} = \{[a], a \in A\}$$

Esempio:
Prendiamo "essere coniugi a modulo 2", gli elementi possono essere o solo pari o solo dispari (quindi appartenere alla classe $[0]$ o alla classe $[1]$)

Definizione di Partizione: Sia A un insieme, una partizione di A è una collezione di sottoinsiemi di A non vuoti a due a due disgiunti, la cui unione è A. A questo punto A può essere rappresentato come l'insieme di tutte le parti:
$A = \{A : i, \in I\}$ dove I rappresenta l'insieme dei contatori
Ogni sottoinsieme gode delle seguenti caratteristiche:

- $A_i \neq \varnothing, \forall i \in I$;
- $A_i \cap A_j = \varnothing, \forall i \neq j$;
- $\bigcup\limits_{i \in I} A_i = A$

Osservazione: Data una relazione di equivalenza, l'insieme delle classi di equivalenza costituisce una partizione di A (per tutti i motivi precedenti). Viceversa, data una partizione $A = \{A_i, \forall i \in I\}$, appartenere allo stessi A_i è una relazione di equivalenza.

Esempio:
Sia $A = \mathbb{Z}$ con la Relazione di Equivalenza essere congrui ad a con modulo n . L'insieme $A_{/\sim}$ può essere indicato con $\mathbb{Z}_{/n}$ per cui:
$\mathbb{Z}_{/n}$= Relazione di Equivalenza di essere congrui ad a di modulo n
Con $n = 2$ si ha che $\mathbb{Z}_{/2} = \{[0]; [1]\}$
Con $n = 3$ si ha che $\mathbb{Z}_{/3} = \{[0]; [1]; [2]\}$
Con qualsiasi n si ha che $\mathbb{Z}_{/n} = \{[0]; [1]; [2]; \ldots; [n-1]\}$

Collegamento tra qualsiasi funzione/relazione: Siano X, Y due insiemi, una relazione $f \subseteq X \times Y$ (funzione interpretata come relazione) è una funzione o una applicazione se:

$$\forall x \in X, \exists! y \in Y : (x, y) \in f$$

In questo caso si scrive $y = f(x)$ oppure $f : X \to Y$

Osservazione: Normalmente una relazione di questo genere viene chiamata "Applicazione", ma se si ha che $Y \sim \mathbb{R}/\mathbb{R}^2$ allora viene definita "Funzione"

Definizione di Funzione Iniettiva: Un'applicazione $f : X \to Y$ è definita "Iniettiva" se "ad elementi diversi sono associati elementi diversi", cioè che se $f(a') = f(a) \Rightarrow a' = a$

Esempio:
$f : \begin{matrix} \mathbb{Z} \to \mathbb{Z} \\ a \mapsto 2a \end{matrix}$ $f(a) = 2a$ è una funzione iniettiva

Definizione di Immagine: Dati $f : X \to Y$, si può definire l'Immagine di f:

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

"Gli elementi di y che vengono da qualche elemento di X"

Definizione di Funzione Suriettiva: Un'applicazione $f : X \to Y$ è definita "Suriettiva" se $Y = Im(f)$

Esempio:
$p : \begin{matrix} \mathbb{R} \to \mathbb{R} \\ (x; y) \mapsto x \end{matrix}$ $p(x, y) = x$ è una proiezione
$\pi : \begin{matrix} A \to A_{/\pi} \\ a \mapsto [a] \end{matrix}$ π è una trasformazione canonica (suddivisione in classi)

Definizione di Funzione Biettiva: Un'applicazione $f : X \to Y$ è biunivoca se è Suriettiva e Iniettiva, cioè se per ogni $y \in Y$ esiste ed è unico $x \in X$ tale che $f(x) = y$. In questo caso è definita anche l'applicazione inversa tale che:
$f^{-1} : \begin{matrix} Y \to X \\ y \mapsto f^{-1}(y) \end{matrix}$, ossia che $x \in X$ è l'unico x tale che $y = f(x)$

Esempi:
$d : \begin{matrix} X \to X \\ x \mapsto x \end{matrix}$
$g : \begin{matrix} \mathbb{Z} \to \mathbb{Z} \\ a \mapsto a+1 \end{matrix} \Leftrightarrow g^{-1} : \begin{matrix} \mathbb{Z} \to \mathbb{Z} \\ b \mapsto b-1 \end{matrix}$

Definizioni di Composizioni: Dati gli insiemi X, Y, Z e le funzioni $f : X \to Y$ e $g : Y \to Z$ e si ha che

$$X \xrightarrow{f} Y \xrightarrow{g} Z \Rightarrow x \mapsto f(x) \mapsto g(f(x))$$

allora è possibile comporle: $g \circ f : X \to Z$ oppure $z = g(f(x))$ o $z = g \circ f(x)$

Osservazione: Se si ha che $f : X \to Y$ è biunivoca allora:

- $f^{-1} \circ f$ è un'identità di x
- $f \circ f^{-1}$ è un'identità di y

Osservazione: In generale la composizione non è biunivoca

Esempio:
$f(x) = 2x \quad g(x) = x+1 \quad g \circ f \neq f \circ g$

Esempi di funzioni Suriettive e non e Iniettive e non (su $f(x) = x^2$):
$f_1 = \mathbb{R} \to \mathbb{R}$ non iniettiva né suriettiva
$f_2 = [0; +\infty) \to \mathbb{R}$ solo iniettiva
$f_3 = \mathbb{R} \to [0; +\infty)$ solo suriettiva
$f_4 = [0; +\infty) \to [0; +\infty)$ biettiva
(Tutto sta nel cambiare il dominio e il codominio)

Posso "curare" la mancanza di Suriettività di una funzione $f : X \to Y$ "sostituendo" y con $f(x)$
Posso "curare" la mancanza di Iniettività di una funzione $f : X \to Y$ "identificando" tra loro elementi che vanno nella stessa y: introduco quindi una relazione di equivalenza $x1 \sim x2 \Leftrightarrow f(x1) = f(x2)$ e sostituisco X con $X_{/\sim}$.

Esempio:
$f : \begin{matrix} X \to Y \\ x \mapsto f(x) \end{matrix}$
Con le trasformazioni π e J diventa
$f : \begin{matrix} X_{/\sim} \to Im(f) \\ [x] \mapsto f(x) \end{matrix}$

Numeri

Definizioni e assiomi di numeri:
Per poter spiegare nell'effettivo cosa sono i numeri vi sono due approcci:

- uno più rapido, ossia direttamente l'assioma dei numeri reali;
- uno più macchinoso, iniziando prima dai numeri naturali, per passare poi a quelli interi, poi razionali, poi reali e poi complessi.

Definizione di Insieme dei Numeri Naturali: (Definiti attraverso l'assioma di Peano)
I numeri naturali sono il dato di:

- un insieme $\mathbb{N}$;
- una applicazione (o funzione) iniettiva $\sigma : \mathbb{N} \to \mathbb{N}$;
  tale che valga la seguente proprietà:
- se $U \subseteq \mathbb{N}$ che contiene 0 e tale che $\forall k \in U, \sigma(k)$ allora $U = \mathbb{N}$
  Si postula quindi che esista una terna $(\mathbb{N}, \sigma, 0)$ con questa proprietà, di dimostrache è essenzialmente unica. In

caso ce ne fosse un'altra, questa sarebbe in biezione con $(\mathbb{N}, \sigma, 0)$

Ogni numero quindi può essere definito come:
$1 = \sigma(0); \quad 2 = \sigma(1) = \sigma(\sigma(0))$

È possibile definire $+$, all'interno dell'insieme $\mathbb{N}$ (dimostrabile per ogni elemento tramite delle dimostrazioni per induzione - se zero gode di determinate proprietà (o qualsiasi elemento k gode di determinate proprietà, allora $k+1$ gode delle stesse proprietà) allora qualsiasi elemento in $\mathbb{N}$ gode delle stesse proprietà), però non è possibile definire la sottrazione. (Tanto che neanche i Greci avevano un concetto di negativo o di sottrazione, essendo la loro matematica legata al mondo naturale e concreto).

Definizione di numeri interi: Su $\mathbb{N} \times \mathbb{N} = \{(a,b), a, b \in \mathbb{N}\}$ introduciamo la Relazione di Equivalenza $(a,b) \sim (a', b')$ se $a + b' = b + a'$ Il che equivarrebbe a dire $a - b = a' - b'$ ma non essendo ancora il segno $-$ qualcosa di concreto si evita.
A questo punto definiamo l'insieme $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})_{/\sim} = \{[(a,0)], a \in \mathbb{N}\} \cup \{[(0,b)], b \in \mathbb{N}, b \neq 0\}$
a questo punto possiamo considerare $(a,0) = a$ e $(0,b) = -b$ quindi $\mathbb{Z} = \{0; 1; 2; 3; \dots\} \cup \{-1; -2 : -3; \dots\}$

Definendo le operazioni in modo usuale: $\mathbb{Z}$ è un "anello commutativo", ossia l'insieme che gode di certe proprietà: operazioni $+$, godono di proprietà associative, commutative, con elementi neutri 0 e 1 e legate dalla proprietà distributiva (come in $\mathbb{N}$), in $\mathbb{Z}$ ogni elemento $a \in \mathbb{N}$ ha un suo opposto $-a$ tale che $a + (-a) = 0$

Tutto ciò da la possibilità di fare le sottrazioni, ma non le divisioni

Definizione di Numeri Razionali:Per poter parlare di frazioni bisogna comunque partire dall'insieme $\mathbb{Z}$.
Dato l'insieme $\mathbb{Z} \times \mathbb{Z} \setminus \{0\} = \{(p,q) \quad t.c. \quad p \in \mathbb{Z}, q \in \mathbb{Z} \setminus \{0\}\}$ pongo la relazione di equivalenza
$(p,q) \sim (q,p) \Leftrightarrow p \cdot q' = q \cdot p'$
A questo punto indico con $p \cdot q = [(p,q)]$ e definisco le operazioni nel modo usuale:
$\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z})_{/\sim}$, dove $\mathbb{Q}$ è un campo, cioè un anello commutativo con la proprietà aggiuntiva che
$x \in \mathbb{Q} \wedge x \neq 0 : x^{-1} \in \mathbb{Q} \Rightarrow x \cdot x^{-1} = 1$ con $x = p/q$ con $p, q \neq 0$

Tutto ciò era stato scoperto da Pitagora nel mondo delle relazioni tra le note musicali:
$\frac{1}{2}$ *corda equivale ad una nota dell'ottava successiva;*
$\frac{1}{2}$ *corda equivale ad una distanza di quinta;*
$\frac{8}{9}$ *corda equivale invece al tono successivo*

Lo stesso Pitagora disse che il numero è la legge razionale dell'universo, non facendo testo del fatto che $\sqrt{2}$ non è razionale.

Definizione di Numeri Reali: Per poter spiegare i numeri reali, bisogna ricorrere alla sequenza di numeri razionali di Cauchy per cui $C = \{\text{Sequenza di numeri razionali}\} = a \cdot n \in \mathbb{Q},\ n \in \mathbb{N}$. Poniamo poi la relazione di equivalenza tra $a \cdot n \sim b \cdot n$ se $\lim_{n \to \infty} (a \cdot n - b \cdot n) = 0$, ponendo poi che $\mathbb{R} = C_{/\sim}$.

Ponendo i numeri in quest'ottica si ha che ogni numero razionale rappresenta una classe di una successione di numeri:

Esempi:
$\pi = [3; 3,1; 3,14; 3,141; \dots]$
$1 = [1; 1; 1; 1; \dots]$
$\frac{1}{3} = [0; 0,3; 0,33; 0,333; \dots]$
$0,\bar{9} = [0; 0,9; 0,99; 0,999; \dots]$
Tuttavia si può notare come le successioni di $0,\bar{9}$ e di 1 sono talmente vicine che sono in relazione, quindi $0,\bar{9} = 1$

Si può quindi affermare che $\mathbb{R}$ è un campo, in quanto gode delle stesse proprietà di $\mathbb{Q}$.
Più nello specifico è possibile affermare che $\mathbb{Q}$ è un sottoinsieme a sé stante di $\mathbb{R}$ in quanto in $\mathbb{R}$ è possibile fare le quattro operazioni, le radici e i limiti.

Però è anche vero che in $\mathbb{R}$ non si possono risolvere equazioni di secondo grado del tipo:
$x^2 + 1 = 0$

Definizione di Insieme dei Numeri Complessi: Per poterla risolvere è possibile inventare un "numero immaginario" i tale che $i^2 = -1$
Dopo questa premessa si vuole comunque poter eseguire tutte le operazioni, quindi:

$\mathbb{C} = \{a + b \cdot i,\ a, b \in \mathbb{R}\}$ = Insieme dei numeri Complessi
È un campo in quanto è possibile poter applicare addizioni (come si fanno tra polinomi), moltiplicazioni (come si fanno tra polinomi), esiste un opposto ($a + b \cdot i - (a + b \cdot i) = 0$) ed esiste un inverso ($(a + b \cdot i) \cdot \frac{a - b \cdot i}{a^2 + b^2} = 1$).

Miracolo Teorema fondamentale dell'Algebra: Ogni equazione polinomiale a coefficienti $\mathbb{C}$ ha soluzione in $\mathbb{C}$ (è un campo algebricamente chiuso, ossia tutto ha soluzioni)

Esistono altre tipologie di insiemi numerici per esempio: Dato $n > \mathbb{N}$, $n > 1$ si ha che:

$$Z_{/n} = \{[0]; [1]; [2]; \ldots; [n-1]\}$$

È possibile rendere quest'insieme un anello attraverso l'inserimento delle operazioni $+, \cdot$

Proposizione: Le operazioni $+, \cdot$ sono ben definite, cioè non dipendono dalla scelta del rappresentante.
Dimostrazione:
(+): Siano $a', b' \in \mathbb{Z}\ t.c.\ [a] = [a']\ e\ [b] = [b']$. Voglio dimostrare che $[a + b] = [a' + b']$
$[a] = [a'] \Rightarrow a \sim a'\ (n) \Rightarrow n | a - a' \Rightarrow \exists k \in \mathbb{Z}\ t.c.\ a' = a + k \cdot n$
$[b] = [b'] \Rightarrow b \sim b'\ (n) \Rightarrow n | b - b' \Rightarrow \exists h \in \mathbb{Z}\ t.c.\ b' = b + h \cdot n$
Dunque si ha che: $a' + b' = a + b + k \cdot n + h \cdot n \Rightarrow a' + b' = a + b + n \cdot (h + k) \Rightarrow$
$n | (a + b) - (a' - b') \Rightarrow (a + b) \sim (a' + b') \Rightarrow [a + b] = [a' + b']$
($\cdot$) (Sul foglio 2 di esercizi)

Quindi $\mathbb{Z}_{/n}$ con le operazioni $+, \cdot$ appena definite è un anello, con elementi neutri $[0]$ e $[1]$, ed elementi opposti: l'opposto di $[a]$ è $[-a] = [n - a] \forall a \in \mathbb{Z}$.
È un campo? Dipende se n è primo o meno

Esempi:
$\mathbb{Z}_{/5} = \{[0]; [1]; [2]; [3]; [4]\}$
$[0]$ non può avere inversi
$[1]$ è inverso di sé stesso
$[2] \cdot [3] = [6] = [1]$ sono inversi tra loro
$[4] \cdot [4] = [16] = [1]$ è inverso di sé stesso
$\mathbb{Z}_{/5}$ è campo

$\mathbb{Z}_{/6} = \{[0]; [1]; [2]; [3]; [4]; [5]\}$
$[2] \cdot [0] = [0]$
$[2] \cdot [1] = [2]$
$[2] \cdot [2] = [4]$
$[2] \cdot [3] = [6] = [0]$
$[2] \cdot [4] = [8] = [2]$
$[2] \cdot [5] = [10] = [4]$
Quindi $Z_{/6}$ non è campo perché $[2]$ non ha inversi, così come $[3]$ e $[4]$.

Osservazione: Se n non è primo allora $\mathbb{Z}_{/n}$ non è un campo (dimostreremo poi perché)

Definizione di Dominio di Integrità: Un anello è un dominio di integrità se $x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$

Esempio:
$\mathbb{Z}$ lo è
$\mathbb{Z}_{/6}$ non lo è

Proposizione: Ogni campo in $\mathbb{K}$ è un dominio di integrità
Dimostrazione:
sia $x \cdot y = 0$ e suppongo $x \neq 0$, allora: $\exists x^{-1} \in \mathbb{K} : x \cdot x^{-1} = 1 \Rightarrow x \cdot x^{-1} \cdot y = 0 \cdot x^{-1} \Rightarrow y = 0$.

Definizione di Caratteristica: Dato un $\mathbb{K}$, definiamo la sua caratteristica, ponendo $1 + 1 + 1 + 1 + 1 + \ldots$ possiamo avere due risultati :

- non ottengo mai 0;
- eventualmente ottengo 0;
  In insiemi come $\mathbb{N}/\mathbb{Z}/\mathbb{Q}/\mathbb{R}$ non ottengo mai 0. In questo caso si dice che $\mathbb{K}$ contiene una "copia" di $\mathbb{Z}$ (anello) e di conseguenza una "copia" di $\mathbb{Q}$ (campo). Si può dire che la caratteristica di $K = 0$.

In insiemi come $\mathbb{Z}_{/p}$ si ottiene 0 dopo p volte. In questo caso si dice che $\mathbb{K}$ contiene una "copia" di $\mathbb{Z}_{/p}$ e diremo che la caratteristica di $K = p$

Dato un qualsiasi numero, per esempio $3784,536$, lo si può scrivere come:
$3 \cdot 10^3 + 7 \cdot 10^2 + 8 \cdot 10^1 + 4 \cdot 10^0 + 5 \cdot 10^{-1} + 3 \cdot 10^{-2} + 6 \cdot 10^{-3}$
Ossia come somma delle varie cifre per una potenza di 10: $\sum_{i=n}^{\ell} C_i \cdot 10^i$
Tutto ciò è legato al fatto che siamo abituati al fatto che usiamo un sistema di calcolo legato alla base decimale, ma lo si potrebbe fare per qualsiasi base b con $\forall b \in \mathbb{N}, b < 1$, in questo caso si avrebbe un insieme delle cifre $b = \{0; 1; 2; \ldots; b-1\}$.
Anche il fatto che un numero si possa definire come finito o infinito dipende dalla base che si prende:

Esempio:
$\frac{1}{2} = 0,5_{10} = 0,\overline{1}_3 \qquad \frac{1}{3} = 0,\overline{3}_{10} = 0,1_3$
Questo perché 2 è un divisore di 10, mentre 3 no
Al contrario, 3 è un divisore di 3, mentre 2 no

Parlando sempre di basi dei numeri, anche i criteri di divisibilità dipendono strettamente dal fatto che usiamo una base 10.

Esempio:
Un numero è multiplo di 9 se la somma delle sue cifre è multiplo di 9
La cosa è strettamente legata al fatto che 9 è un numero vicino a 10
$10 \equiv 1\ (9) \qquad 10^2 \equiv 1\ (9) \qquad \sum_{i=1}^{n} n \equiv C_i\ (9)$
Più specificamente, un numero è divisibile per 9 se è congruo alla somma delle sue cifre.
La cosa si può definire simile per 11, ma bisogna alternare in ogni cifra fra la cifra stessa e il suo opposto:
$\sum_{i=1}^{n} n \equiv (-1)^i \cdot C_i\ (11)$
Poi per 2 e 5 è necessario vedere l'ultima cifra: basta che sia multiplo di 2 $(0; 2; 4; 6; 8)$, oppure multiplo di 5 $(0; 5)$.
Questo perché sono 2 e 5 sono divisori di 10.

Definizione di Cardinalità di un insieme finito: Dato un insieme A, possiamo definire la sua Cardinalità $|A|$ il numero dei suoi elementi.

Combinatoria

Esempio:
Dati due insiemi X e Y possiamo definire le loro cardinalità $|X| = m$, $|Y| = n$. Siano per esempio gli insiemi X e Y con $|X| = m = 3$ e $|Y| = n = 5$, quante applicazioni si possono definire?
Visto che per ogni elemento di X ho a disposizione 5 possibilità e ho 3 elementi, allora ho: $5 \cdot 5 \cdot 5 = 5^3 = 125$

Definendo un caso più generale ho $|Y|^{|X|} = n^m$ possibilità.

Esempio pt.2
Se le applicazioni dovevano essere iniettive, allora:
- per il primo elemento avrei avuto 5 possibilità;
- per il secondo elemento 4 possibilità;
- per il terzo, 3;
Quindi sarebbe stato $5 \cdot 4 \cdot 3$

Definendo più in generale, si possono distinguere 3 casi

- se $m < n = \dfrac{n!}{(n-m)!}$
- se $m = n$ (quindi biunivoche) $=n!$
- se $m > n = 0$ (in questo caso non ci sarebbe stata l'iniettività)

Lavorando con gli insiemi, abbiamo visto che dato un insieme A di n elementi, allora $|\mathcal{P}(A)| = 2^n$. Riprendendo un sistema iniziale di domande per vedere se ci sono gli elementi o meno in ogni sottoinsieme S è possibile creare una

sequenza di 0 e 1 (dove 0 corrisponde a "non è presente" e 1 a "è presente"). In questo modo nasce una biezione tra $\mathcal{P}(A)$ e S^n:
$\begin{array}{ccc} \mathcal{P}(A) & \to & S^n \\ x & \mapsto & c_i \dots c_n \end{array}$ dove $c_i = 1$ se $i \in A$ e $c_i = 0$ se $i \notin A$

Esempio:
Quanti insiemi si possono creare con la stessa cardinalità?
Supponiamo di avere un insieme A di 5 elementi e si vuole sapere quanti sottoinsiemi S si possono creare di cardinalità 3. Si ha che per il primo elemento ci sono 5 scelte, per il secondo 4 scelte e 3 per il terzo, per un totale di 60 scelte. Però bisogna anche togliere tutti gli insiemi contati diverse volte.

Per creare un caso più generale, se $|A| = n$ e $|S| = k$ con $(0 \leq k \leq n)$ si ha che
$\frac{n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-k+1)}{k \cdot (k-1) \cdot (k-2) \cdot \ldots \cdot (1)} = \frac{n!}{(n-k)! \cdot k!}$
Quest'ultimo si chiama Coefficiente binomiale e può essere scritto anche come:

$$\binom{n}{k}$$

Sia $S_{nk} = \{\text{Sottoinsiemi di } \{1, 2, \ldots, n\} \text{ con } k \text{ elementi}\}$ e sia
$S^{nk} = \left\{ \text{Successioni di } c_1, c_2, \ldots, c_n, c \in \{0; 1\} \text{ con } k \mid \sum_{i=1}^{n} c_i = k \right\}$, allora c'è una biezione.
$\begin{array}{c} S_{nk} \to S^{nk} \\ x \mapsto c_i \dots c_n \end{array}$ dove $c_i = 1$ se $i \in A$ e $c_i = 0$ se $i \notin A$

Proprietà: $\binom{n}{k} = \binom{n}{n-k}$
Si potrebbe dire con estrema semplicità che $\frac{n!}{(n-k)! \cdot k!} = \frac{n!}{k! \cdot (n-k)!}$, ma non è una dimostrazione illuminante, quindi: Si definisce un'applicazione $c : \begin{array}{c} S_{n,k} \to S_{n,n-k} \\ X \to A \setminus X \end{array}$. c è direttamente biunivoca (ogni sottoinsieme ha un complementare), quindi $\binom{n}{k} = |S_{n,k}| = |S_{n,n-k}| = \binom{n}{n-k}$

Proprietà: $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ (Triangolo di Tartaglia)
Dimostrazione:
$S_{n,k} = \{X \subseteq A |\ |X| = k\}$. Questo insieme può essere scritto come l'unione di due insiemi complementari
$S_{n,k} = \{X \subseteq A |\ |X| = k, n \notin X\} \cup \{X \subseteq A |\ |X| = k, n \in X\}$ ^1149df
A partire da questi sottoinsiemi possiamo crearne altri con cardinalità diversa:
$S_{n,k} = \{X \subseteq \{1, 2, \ldots, n-1\} |\ |X| = k\} \cup \{X \subseteq B \cup \{n\}, B \subseteq \{1, 2, \ldots, n-1\}, |B| = k-1\}$
$S_{n,k} = S_{n-1,k} \{B \cup \{n\}, B \in S_{n-1,k-1}\}$

Questo è lo stesso concetto di $(x+y)^n = (x+y)(x+y) \ldots (x+y) = \sum a_i \cdot x^i \cdot y^{n-i}$, dove a_i rappresenta il numero di successioni di lunghezza n che contengono i volte x e $n-1$ volte y. Quindi si ottiene $a_i = \binom{i}{n} = |S_{n,i}|$

Esempi di esercizi:
1. In quanti modi posso dare C caramelle a b bambini?
Il numero di bambini corrisponde al numero di sbarrette $+1$, quindi il numero di sbarrette è $b-1$. A questo punto si può vedere come una sequenza di uno e zero tale che $1 =$ numero di caramelle e $0 =$ numero di sbarrette, in questo modo $S_c^{c+b-1} = \binom{c}{c+b-1}$
2. Quante soluzioni $x \in \mathbb{N}$ ha l'espressione $x_1 + x_2 + \ldots + x_b = c$?
Stessa identica cosa di sopra.
3. In un percorso 5×3, quanti sono i modi possibili in modo da fare il numero di passi minimi?
Si ha che la lunghezza minima è uguale a 8 con 5 in una direzione e 3 nell'altra, quindi $\binom{3}{8} = \binom{5}{8}$

Definizione di ragionamento per induzione: "Se è vero per n, allora è vero per n+1"

Esempio:
$n^2 = \sum_{k=1}^{n} (2k-1) \Rightarrow n^2 + (2n+1) = \sum_{k=1}^{n} (2k-1) + (2n) + 1 \Rightarrow (n+1)^2 = \sum_{k=1}^{n+1} (2k-1)$

Definizione di Cardinalità: Due insiemi A e B hanno la stessa Cardinalità se esiste una biezione $A \to B$.
Per gli insiemi finiti si guarda il numero di elementi, per quelli infiniti invece se è presente una biezione con insiemi infiniti.

Osservazione: Essere in biezione è una relazione di equivalenza (primo foglio di esercizi).

Esempio:
L'insieme $\mathbb{Z}$ e $2\mathbb{Z}$ (l'insieme dei numeri pari) sono in biezione tra di loro perché ad ogni numero posso associare il suo doppio. *Può sembrare un paradosso, in quanto insiemisticamente $2\mathbb{Z}$ ha metà degli elementi. Eppure c'è biezione, in quanto ad ogni elemento del primo è associato uno e uno solo elemento del secondo*

Definizione: Diciamo che un insieme A ha cardinalità minore o uguale di un insieme B se esiste una applicazione biettiva da A a B

Esempio:
$card(\mathbb{N}) \leq card(\mathbb{R})$ per $\begin{matrix} \mathbb{N} \to \mathbb{R} \\ n \mapsto n \end{matrix}$

Teorema (CBS): Se $card(A) \leq card(B)$ e $card(B) \leq card(A) \Rightarrow card(A) = card(B)$. Ovvero se esistono due applicazioni iniettive $f : A \to B$ e $g : b \to A$, allora esiste una biezione tra A e B

Esempio:
Sia $A = [0, 1]$ e $B = [0, 1[$ e siano $A \underset{f,g}{\overset{f,g}{\longleftrightarrow}} B$ con $f(x) = \frac{x}{2}$ e $g(x) = x$ con f, g iniettive
Si ha che esiste una funzione h definita come $h : \begin{cases} \frac{x}{2} & \text{se } x = 2^{-n}, n \in \mathbb{Z} \\ x & \text{altrimenti} \end{cases}$, quindi $[0, 1]$ e $[0, 1[$ sono in biezione per h

Definizione di Numerabile: Un insieme è definito numerabile se ha la stessa cardinalità di $\mathbb{N}$

Osservazione: Se A è numerabile, possiamo elencare i suoi elementi con termini di una successione, cioè $A = \{a_0, a_1, a_2, \dots\} = \{a_n \wedge n \in \mathbb{N}\}$. *(Se A è un insieme finito di elementi si ha che al posto di $\mathbb{N}$, si ha un insieme $N \subseteq \mathbb{N}$)*

Esempio:
Si ha che $\mathbb{Z}$ è numerabile, perché mettendolo nella successione $0, 1, -1, 2, -2, \dots$ ad ogni numero in $\mathbb{Z}$ è associato uno un solo elemento di A_n:
$0 = a_0, 1 = a_1, -1 = a_2, 2 = a_3, 2 = a_4, \dots$

Teorema: Il prodotto cartesiano di due insiemi è numerabile
Dimostrazione:
Siano A e B due insiemi numerabili tale che $A = \{a_n, n \in \mathbb{N}\}$ e $B = \{b_n, n \in \mathbb{N}\}$.
Si ha che ogni elemento (a_n, b_n) può essere scritto come in una tabella:

$$\begin{matrix} (a_0, b_0) & (a_0, b_1) & (a_0, b_2) & \dots \\ (a_0, b_0) & (a_0, b_1) & (a_0, b_2) & \dots \\ (a_2, b_0) & (a_2, b_1) & (a_2, b_2) & \dots \\ \vdots & \vdots & \vdots & \ddots \end{matrix}$$

Si possono tracciare delle Diagonali in modo che intersechino i punti nel seguente modo:
$d_0 : (a_0, b_0); \quad d_1 : (a_1, b_0) - (a_0, b_1); \quad d_2 : (a_2; b_0) - (a_1, b_1) - (a_0, b_2)$, e così via.
Seguendo quest'ordine posso associare un $n \in \mathbb{N}$ ad ogni coppia:
$c_0 : (a_0, b_0); \quad c_1 : (a_1, b_0); \quad c_2 : (a_0, b_1)$, eccetera.
Visto che il prodotto cartesiano è un insieme finito, si ha che tutte le diagonali insieme sono in grado di prendere ogni coppia, quindi ogni elemento è coperto. Di conseguenza ho enumerato tutti gli elementi di $A \times B$.

Osservazione: Per induzione possono mostrare che se da A_1 a A_n sono insiemi numerabili, allora $A_1 \times A_2 \times A_3 \times \dots \times A_n$ è numerabile.

Corollario: $\mathbb{Q}$ è numerabile
Dimostrazione:
Si può interpretare $\mathbb{Q}$ come $\frac{\mathbb{Z} \times \mathbb{Z} \setminus \{0\}}{/\sim}$, poi si crea una tabella simile alla precedente Algebra 1 - Moci > ^41cbb2, in cui le entrate sono i numeratori e i denominatori. Si tracciano poi le diagonali (tutto similmente a prima) e si prendono solo le frazioni che portano a risultati diversi ($\frac{2}{4}$ non si prende per esempio). Poi si procede in maniera analoga a prima.

Corollario: $\mathbb{Z}^n$ e $\mathbb{Q}^n$ sono numerabili ($\forall n \in \mathbb{N}, n > 0$)

Teorema: L'insieme di una infinità di insiemi numerabili è numerabile
Dimostrazione:
Siano $A_0, A_1, A_2, \ldots$ insiemi numerabili. Ognuno di questi si può scrivere come $\forall n \in \mathbb{N} \quad A_n = \{a_{n0}, a_{n1}, a_{n2}, \ldots\}$, allora posso creare una tabella simile a quella di prima Algebra 1 - Moci > ^41cbb2, dove le entrate sono il numero dell'inisieme e il numero dell'elemento.
Così facendo ottengo un insieme tale che: $A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_n = \bigcup\limits_{n \in \mathbb{N}} A_n$

Sia A un insieme numerabile e consideriamo l'insieme B di tutte le successioni degli elementi di A di lunghezza finita. In altre parole, consideriamo l'insieme A come l'insieme "alfabeto" e l'insieme P come le "parole".

Corollario: P è numerabile.
Dimostrazione:
$P = \bigcup_{n \in \mathbb{N}} P_n$, dove P_n rappresenta l'insieme di tutte le parole P di lunghezza n. Si ha tuttavia che $P_n = A^n = A \times A \times A \times \ldots \times A$, n volte $\Rightarrow$ P_n è numerabile$\Rightarrow$ P è numerabile.

Insieme di Cantor:

$$C = \{x \in [0, 1[\mid \text{in base 3},\ x = c_1 c_2 c_3 \ldots\ c_i \in \{0; 2\}\}$$

L'insieme di Cantor è l'insieme che contiene tutti i numeri decimali compresi tra 0_3 e 1_3 tali che non contengono la cifra 1. La rappresentazione grafica è quella di un frattale.

Definizione di Insieme Non Numerabile: Un insieme si definisce non numerabile se non è possibile stabilire una biezione con $\mathbb{N}$.

Teorema: Sia A un insieme, allora $card(A) < card(\mathcal{P}(A))$. *$\leq$ implica che c'è una biezione, $\neq$ implica che non c'è biezione*
Dimostrazione:
Dobbiamo dimostrare che $\exists g : A \to \mathcal{P}(A)$ iniettiva e $\nexists f : A \to \mathcal{P}(A)$.
$g :^{A \to \mathcal{P}(A)}_{a \to \{a\}}$ è iniettiva e non suriettiva, ma non mi basta per dire che non c'è biezione
Sia $f : A \to \mathcal{P}(A)$, definisco un insieme $D = \{a \in A | a \notin f(A)\}$, quindi si ha che $\forall a \in A :^{a \in D, a \notin f(A)}_{a \notin D, a \in f(A)}$.
Da ciò si giunghe che D non è $f(A)$ per nessun $a \in A$, cioè $D \in Imf$, quindi f non è suriettiva, quindi non c'è biezione
Conseguenza: esistono infinite cardinalità infinite, cioè $card(A) < card(\mathcal{P}(A)) < card(\mathcal{P}(\mathcal{P}(A))) < \ldots$.

Definizione di Sucessione Binarie e Infinite: $\{0; 1\}^{\mathbb{N}} = \{\text{Sucessioni } a_n, n \in \mathbb{N}, a_n \in \{0; 1\}\}$

Teorema: $\{0; 1\}^{\mathbb{N}}$ non è numerabile
Dimostrazione:
Supponiamo per assurdo che lo sia: si può scrivere allora $\{0; 1\}^{\mathbb{N}}$ come un insieme di sequenze $\{S_0, S_1, S_2, S_3, \ldots\} = \{S_n, n \in \mathbb{N}\}$. Di conseguenza le si possono rappresentare come una tabella (simile a Algebra 1 - Moci > ^41cbb2)

$$\begin{array}{ccccc}
(a_{00}) & (a_{01}) & (a_{02}) & \ldots & (S_0) \\
(a_{10}) & (a_{11}) & (a_{12}) & \ldots & (S_1) \\
(a_{20}) & (a_{21}) & (a_{22}) & \ldots & (S_2) \\
\ldots & \ldots & \ldots & & \ldots
\end{array}$$

In questo modo si ha che tutti gli elementi di $\{0; 1\}^{\mathbb{N}}$ sono stati rappresentati.
Adesso possiamo definire una sequenza $d \in \{0; 1\}^{\mathbb{N}}$ in questo modo: $d = \begin{cases} 0\ se\ a_{ii} = 1 \\ 1\ se\ a_{ii} = 0 \end{cases}$
Quindi si giunge che $d \in \{0; 1\}^{\mathbb{N}}$, ma $d \neq S_i, \forall i \in \mathbb{N}$ (qui cade l'assurdo)

Osservazione: $\mathcal{P}(\mathbb{N})$ è in biezione con $\{0; 1\}^{\mathbb{N}}$, infatti $A \mapsto S_a = a_0 a_1 a_2 \ldots, a_i = \begin{cases} 1 \in A \\ 0 \notin A \end{cases}$
Chiaramente si ha che con sottoinsiemi diversi si ottengono successioni diverse. Inoltre fornisce un'altra dimostrazione del fatto che $\mathcal{P}(N)$ non è numerabile

Teorema: $\{0; 1\}^{\mathbb{N}}$ è in biezione con l'insieme di Cantor e quindi non è numerabile
Dimostrazione:

È sufficiente sostituire gli 1 con i 2

$f: \begin{matrix} \{0;1\}^{\mathbb{N}} & \to & C \\ \substack{S=a_0a_1a_2\dots \\ a_i\in\{0;1\}} & \mapsto & \substack{x=c_0c_1c_2\dots \\ c_i=\substack{0\ se\ a_i=0 \\ 2\ se\ a_i=1}} \end{matrix}$ si ha quindi che f è chiaramente biunivoca

Teorema: L'intervallo $]0;1[$ non è numerabile ed ha la stessa cardinalità di $\{0;1\}^{\mathbb{N}}$ e $\mathcal{P}(N)$
Dimostrazione:
Mostriamo che $]0;1[$ è in biezione con $\{0;1\}^{\mathbb{N}}$
$\varphi: \begin{matrix}]0;1[\to \{0;1\}^{\mathbb{N}} \\ n \mapsto c_1c_2c_3 \end{matrix}$ dove $n = 0, c_1c_2\dots, c_i \in \{0;1\}$ in base scritto nella maniera più semplice, (ossia senza l'uso spasmodico del periodico: $1_2 = 0,\overline{1}_2$)
si ha che φ è iniettiva ma non è suriettiva in quanto (per esempio) $0,\overline{1} \notin Im\varphi$, oppure $\frac{1}{2} = 0,1_2 (\in \varphi) = 0,0\overline{1}_2 (\notin \varphi)$.
Tuttavia, come prima, non si può concludere che esiste una biezione tra i due, di conseguenza si opta al teorema CBS (Algebra 1 - Moci > ^a9e21f)
Definiamo quindi: $\psi: \{0;1\}^{\mathbb{N}} \to]0;1[_{\text{in base } 3} = c_0c_1c_2\dots \mapsto 0, b_0b_1b_2\dots$ dove $b_i = \begin{cases} 0\ se\ a_i = 0 \\ 2\ se\ a_i = 1 \end{cases}$, con questo possiamo dire che ψ è insiettiva.
Avendo quindi due funzioni iniettive $\varphi:]0;1[\to \{0;1\}^{\mathbb{N}}$ e $\psi: \{0;1\}^{\mathbb{N}} \to]0;1[$ si ha che, per il teorema CBS, i due insiemi non numerabili sono in biezione.

Teorema: $\mathbb{R}$ è in biezione con $]0;1[$. In particolare $\mathbb{R}$ non è numerabile e $card(\mathbb{R}) = card(\mathcal{P}(\mathbb{N}))$.
Dimsotrazione:
per collegare facilmente un intervallo è $\mathbb{R}$ c'è la funzione $\tan$, solo che l'intervallo desiderato è $]-\frac{\pi}{2}, \frac{\pi}{2}[$. Si possono fare delle trasformaioni (prima traslazione, poi dilatazione) per ottenere l'intervallo desiderato
$]0;1[\Rightarrow]0-\frac{1}{2}; 1[=]-\frac{1}{2}; \frac{1}{2}[\Rightarrow]-\frac{1}{2}\cdot\pi; \frac{1}{2}\cdot\pi[=]-\frac{\pi}{2}; \frac{\pi}{2}[$
Quindi si ha che: $h = \tan \circ g \circ f:]0;1[\to \mathbb{R}$, esiste anche quella inversa: $h^{-1}(y) = \frac{\arctan y}{\pi} + \frac{1}{2}$.

Definizione di Denso: In ogni intervallo di estremi in $\mathbb{Q}$ si ha che ci sono infiniti numeri

---

Congruenze

Definizione di Primo e Irriducibile: Un intero $p \in \mathbb{Z}$ è primo $p \neq 0, -1, 1$ è

1. *primo* se $\forall a, n \in \mathbb{Z}$ t.c. $p | a \cdot b$, si ha che $p | a$ oppure $p | b$
2. *irriducibile* se $\forall a, b \in \mathbb{Z}$ t.c. $p = a \cdot b$ si ha che $a = \pm 1$ oppure $b = \pm 1$
   Queste definizioni corrispondono solamente nell'anello $\mathbb{Z}$, ma non negli altri.

Controesempio:
$12 | 28 \cdot 15$ ma $12 \nmid 28$ e $12 \nmid 15$, quindi non è primo
$12 = 3 \cdot 4$, ma $3 \neq \pm 1$ e $4 \neq \pm 1$, quindi non è irriducibile

Proposizione: Ogni primo è irriducibile
Dimostrazione:
Sia $p = a \cdot b \Rightarrow p | a \cdot b$ (perché $1p = ab$), ma p è primo, quindi $p | ab \Rightarrow p | a$ oppure $p | b$. Non è restrittivo supporre che $p | a$ (in quanto, valendo la proprietà simmetrica, l'uno vale l'altro), cioè $\exists h \in \mathbb{Z}$ t.c. $ph = a \Rightarrow p = ab = phb \Rightarrow hb = 1$, cioè $h = b^{-1}$, ma l'unico numero per cui ciò è valido è con ± 1, quindi $b = \pm 1$.

Proposizione: Siano $a, b \in \mathbb{Z}, b \neq 0$. Allora $\exists! q, r \in \mathbb{Z}$ con $0 < r \leq |b|$ t.c. $a = bq + r$, dove q sta per quoziente e r per resto.

Esempio:
$14/3 = 4$ con resto 2: $14 = 3 \cdot 4 + 2$
$-14/3 = -5$ con resto 1: $-14 = 3 \cdot (-5) + 1$

Dimostrazione:
Per Induzione su $n = |a|$
- Base di induzione: se $n = 0, a = 0$ basta prendere $q = 0$ e $r = 0$
- Passo: Supponiamo l'enunciato $\forall a, b$ t.c. $|a| < n$ e dimostriamo l'enunciato $\forall a, b$ t.c. $|a| = n$
Sia $a, b \in \mathbb{Z}, b \neq 0$ t.c. $|a| = n$
- Se $|a| < |b|$, basta prendere $q = 0$, $r = |a|$ (se $a \geq 0$), $q = -1$, $r = |b| - |a|$ con $a < 0$
- Se $|a| \geq |b|$, si possono distinguere vari casi

- se $a \geq 0$ e $b > 0$ (quindi $a \geq b$). Consideriamo $a' = a - b$ poiché $|a'| < |a| = n$ per l'ipotesi induttiva $\exists! q', r' \in \mathbb{Z}\ 0 < r' < b$ t.c. $a' = bq' + r'$, ma allora $a = a' + b = b + (q' + 1) + r'$, dunque $q = q' + 1$ e $r' = r$ sono gli interi ricercati.
- Se $a < 0, b > 0$, pongo $a' = a + b$, ho che $|a'| < |a| = n$ e posso procedere in modo induttivo come prima.
- Se $b < 0$, ho che $-b > 0$ e quindi $\exists! q, r \in \mathbb{Z}, 0 \leq r < |b|$ t.c. $a = (-b)q + r = b(-q) + r$, quindi $-q$ e r sono i numeri cercati.

Definizione di $\mathcal{MCD}$: Siano $a, b \in \mathbb{Z}$. Diciamo che $d \in \mathbb{Z}$ è un Massimo Comune Divisore ($d = \mathcal{MCD}(a, b)$) se:

- $d|a$ e $d|b$ (d è un divisore comune);
- $\forall d' \in \mathbb{Z}$ t.c. $d'|a$ e $d'|b$ allora $d'|d$ (è il massimo nel senso della divisibilità).

È unico?
Siano $d, e \in \mathbb{Z}$ due numeri che soddisfano le proprietà 1 e 2 della definizione precedente. Per la seconda proprietà si ottiene che $d|e$ e $e|d$, quindi si può concludere che $d = e$
Quindi si, è unico a meno del segno (infatti per $\mathcal{MCD}$ si prende generalmente quello di segno positivo)

Teorema: Siano $a, b \in \mathbb{Z}$, allora esiste $d = \mathcal{MCD}(a, b)$. Inoltre $\exists n, m \in \mathbb{Z}$ t.c. $d = an + bm$ (Identità di Bézout) ^8c61e1
Dimostrazione:
Non è restrittivo supporre $a \geq 0$ e $b \geq 0$, infatti se sono negativi è possibile sostituirli con il loro opposto e il $\mathcal{MCD}$ non cambia. Procediamo per induzione su $m = min(a, b)$. Supponiamo vero l'enunciato $\forall (a, b) \in \mathbb{Z}$ t.c. $min(a, b) < n$ e dimostriamolo con $\forall (a, b) \in \mathbb{Z}$ il $min(a, b) = n$
- Base: Per induzione ($n = 0$), $\mathcal{MCD}(a, 0) = a \Rightarrow d = a$
- Passo: Non è restrittivo supporre che $a \geq b$ (in caso contrario si fa in modo analogo con b). Facciamo la divisione con il resto $a = bq + r,\ 0 \leq r < b$. Per ipotesi induttiva, $\exists d = \mathcal{MCD}(b, r)$. Mostriamo che $d = \mathcal{MCD}(b, r)$
- Poiché $d = \mathcal{MCD}(b, r)$, $d|b$ e $d|r$, allora $d|a = d|bq + r$ (divide la somma di multipli di d)
- Sia $d' \in \mathbb{Z}$ t.c. $d'|a$, $d'|b$, allora $d'|r = d'|a - bq$ (visto che $d = \mathcal{MCD}(b, r)$)$\Rightarrow$ $d'|d$, quindi, $d = \mathcal{MCD}(a, b)$
Quindi $d = \mathcal{MCD}(a, b)$
Sempre per Ipotesi Induttiva, $\exists n', m' \in \mathbb{Z}$ t.c. $n'r + m'b = d$. Sostituendo $r = a - bq$ ottengo $n'(a - bq) + m'b = d \Rightarrow n'a - b(-n'q + m') = d$. $n = n'$ e $m = m' - nq$ sono gli interi cercati.

Come trovare il $\mathcal{MCD}$?
La dimostrazione precedente è costruttiva, cioè è stata creata in modo da fornire un algoritmo (l'algoritmo di Euclide) per calcolare il $\mathcal{MCD}$ e trovare un'identità di Bézout.

Esempio:
Troviamo il $\mathcal{MCD}(4512, 306)$
$4512/306 = 14 \text{ con resto } 228$ cioè $4512 = 306 \cdot 14 + 228$, quindi $d = \mathcal{MCD}(306, 228)$
$306/228 = 1 \text{ con resto } 78 \qquad d = \mathcal{MCD}(228, 78)$
$228/78 = 2 \text{ con resto } 72 \qquad d = \mathcal{MCD}(78, 72)$
$78/72 = 1 \text{ con resto } 6 \qquad d = \mathcal{MCD}(72, 6)$
$72/6 = 12 \text{ con resto } 0 \qquad d = \mathcal{MCD}(6, 0) = 6$
Questo si fa fino a che il resto non diventa 0.
A questo punto è possibile trovare l'identità di Bézout: $6 = 4512n + 306n$
Per fare ciò dobbiamo ricorrere alle divisioni precedenti:
$6 = 78 - 72$, ma si ha che $72 = 228 - 2 \cdot 78$
$6 = 78 - 228 + 2 \cdot 78 = -228 + 3 \cdot 78$, ma si ha che $78 = 306 - 228$
$6 = -228 + 3 \cdot 78 = -228 + 3 \cdot 306 - 3 \cdot 228 = 3 \cdot 306 - 4 \cdot 228$, ma si ha che $228 = 4512 - 14 \cdot 306$
$6 = 3 \cdot 306 - 4 \cdot 228 = 3 \cdot 306 - 4 \cdot 4512 + 56 \cdot 306 = -4 \cdot 4512 + 59 \cdot 306$
Si ha che $n = -4$ e $m = 59$

Dimostrazione:
Sia p irriducibile. Vogliamo dimostrare che $p|ab \Rightarrow p|a$ o $p|b$.
Si ha quindi che $\mathcal{MCD}(a, p) = 1 \vee p$ (essendo irriducibile non ha altri divisori)
Se $\mathcal{MCD}(a, p) = p$, allora si ha che $p|a$ che è la tesi
Se $\mathcal{MCD}(a, p) = 1$, ho l'identità di Bézout: $\exists m, n \in \mathbb{Z}$ t.c. $na + mq = 1$, moltiplicando da entrambe le parti per b ottengo $mab + npb = b$, per Ipotesi ho che $p|ab \Rightarrow p|nab + mbp$ in quanto è una somma di multipli di b, quindi $p|b$, ossia la tesi.

Questo è valido solo per $\mathbb{Z}$, in quanto è possibile fare la divisione con resto, quindi in $\mathbb{Z}$ irriducibile e primo sono la stessa cosa.

Definizione di Equazione Diofantea: Un'equazione si definisce diofantea se è nella forma:

$$ax + by = c \quad a, b, c \in \mathbb{Z}$$

e cerchiamo i valori interi delle incognite x, y

Esempio:
- Esercizio 5 Foglio di Esercizi 3: Foglio 3.pdf
- $4512x + 306y = 18$, qui mi basta moltiplicare l'Identità di Bézout prima ricavata (Algebra 1 - Moci > ^0dbded) ($4512 \cdot (-4) + 306 \cdot 59 = 6$) per 3 e ottengo le soluzioni $x = -4 \cdot 3 = -12;\ y = 59 \cdot 3 = 177$
- $4x + 6y = 13$ non ha soluzioni perché $2 = \mathcal{MCD}(4, 6) \nmid 13$

Abbiamo scoperto che data l'equazione $ax + by = c$ e posto $d = \mathcal{MCD}(a, b)$ ho 2 casi:

- se $d \nmid c$, non ho soluzioni in $\mathbb{Z}$
- se $d | c$, posso ottenere una delle (infinite soluzioni), moltiplicando l'Identità di Bézout ($an + bm = d$) per l'intero $\frac{c}{d}$.

Conseguenza: Così si possono trovare gli inversi in $\mathbb{Z}_{/n}$, infatti possiamo dimostrare il seguente teorema.

Teorema: Sia $n \in \mathbb{N}, n > 1$ e sia $a \in \mathbb{Z}$. $[a] \in \mathbb{Z}_{/n}$ è irriducibile $\Leftrightarrow \mathcal{MCD}(a, n) = \pm 1$.
In particolare $\mathbb{Z}_{/n}$ è un campo $\Leftrightarrow$ n è primo.
Dimostrazione:
$[a]$ è invertibile in $\mathbb{Z}_{/n} \Leftrightarrow \exists x \in \mathbb{Z} : [a] \cdot [x] = [1]$, ma $[x] \cdot [a] = [xa] \Leftrightarrow ax \equiv 1(n) \Leftrightarrow n | ax - 1 \Leftrightarrow \exists y \in \mathbb{Z}$ t.c. $ny = ax - 1 \Leftrightarrow \exists x, y \in \mathbb{Z}$ t.c. $1 = ax - ny$
Se $d = \mathcal{MCD}(a, n) > 1$ non c'è: $d | ax,\ d | ny \Rightarrow d | 1$, la cosa risulta Assurda
Se $d = \mathcal{MCD}(a, n) = 1$, x e y esistono per l'identità di Bézout $\Rightarrow [a]$ è invertibile
Infine notiamo che $\mathbb{Z}_{/n}$ è un campo $\Leftrightarrow [a]$ è invertibile $\forall a \neg \equiv 0(n), a \in \mathbb{Z} \Leftrightarrow \mathcal{MCD}(a, n) = 1,\ \forall a \neg \equiv 0(n) \Leftrightarrow$ n è irriducibile.

Esempio:
Trovare che esiste l'inverso di $[35]$ in $\mathbb{Z}_{/74}$
Si segue il ragionamento di Algebra 1 - Moci > ^0dbded, quindi:
$74 = 35 \cdot 2 + 4;\ 35 = 4 \cdot 8 + 3;\ 4 = 3 \cdot 1 + 1;\ 3 = 1 \cdot 3 + 0$. Quindi $\mathcal{MCD}(74, 35) = 1 \Rightarrow [35]$ è invertibile ma di chi? Bézout: $1 = 4 - 3 = -35 + 4 \cdot 9 = -35 + 9 \cdot (74 - 35 \cdot 2) = 9 \cdot 74 - 19 \cdot 35$. Riducendola a $\mathbb{Z}_{/74}$ diventa $1 = -19 \cdot 35$ cioè in $\mathbb{Z}_{/74}$ $[1] = [-19] \cdot [35]$, quindi l'inverso cercato è $[-19] = [74 - 19] = [55]$

Teorema Fondamentale dell'Aritmetica: Sia $n \in \mathbb{N}, n \geq 2$ allora n si *scrive* come prodotto di numeri primi, in modo *unico* a meno dell'ordine (La cosa è valida solamente in $\mathbb{Z}$)

Osservazione: Su altri anelli la cosa non è verificata.

Esempio:
Sia $\mathbb{Z}[\sqrt{-5}] : \{a + \sqrt{-5}b, a, b \in \mathbb{Z}\}$. $(1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}) = 2 \cdot 3 = 6$ quindi non si scrive in modo unico.

Dimostrazione dell'Esistenza:
Procediamo in modo Induttivo su n:
Base: $n = 2$ è primo, non c'è nulla da dimostrare
Passo: Supponiamo di aver mostrato che ogni $a < n$ si fattorizza come prodotto di primi. Si possono distinguere 2 casi in questo modo
- Se n è primo non c'è nulla da dimostrare
- Se n non è primo allora non è irriducibile $\Rightarrow \exists a, b \in \mathbb{N}$ t.c. $n = ab$, dove $a, b \neq \pm 1$. Poiché $a < n, b < n$ si fattorizza come prodotto di primi $a = p_1 \cdot \ldots \cdot p_n$ e $b = q_1 \cdot \ldots \cdot q_\ell$ quindi $n = a \cdot b = p_1 \cdot \ldots \cdot p_n \cdot q_1 \cdot \ldots \cdot q_\ell$, ciò implica che esiste.
Dimostrazione dell'Unicità:
Supponiamo due fattorizzazioni in fattori primi: $n = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$ (con $r \leq s$) e mostriamo che $r = s$ a meno dell'ordine ($p_1 = q_1, p_2 = q_2 = \ldots = p_r = q_s$). Proseguiamo per induzione su r
- Base: $r = 1 \Rightarrow p_1 = q_1 \cdot \ldots \cdot q_s$, dunque $p_1 | q_1 \cdot q_s \Rightarrow p_1 | q_i$ per qualche i. Non è restrittivo supporre che $p_1 | q_1$, ma q_1 è irriducibile, quindi $p_1 | q_1 \Rightarrow q_2 \cdot \ldots \cdot q_s = 1 \Rightarrow s = 1$
- Passo: $p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$, dunque $p_i | q_1 \cdot \ldots \cdot q_s$ per qualche i. Non è restrittivo supporre che $p_i | q_i$, ma q_i è irriducibile,

quindi $p_i = q_i$. Semplificando $p_i | q_i$ si ottiene $p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot q_s$ lunghi rispettivamente $r-1$ e $s-1$. Per ipotesi induttiva si ha che devono essere la stessa fattorizzazione: $r-1 = s-1$, $p_2 = q_2, \ldots, p_r = q_s$

Osservazione: Nella dimostrazione ho usato varie volte l'equivalenza tra primo e irriducibile

Proposizione (Conseguenza): Se p è primo, allora $\sqrt{p} \notin \mathbb{Q}$
Dimostrazione:
Supponiamo per assurdo che $p = \frac{a^2}{b^2},\ a, b \in \mathbb{Z},\ b \neq 0$
Quindi $p = \frac{a^2}{b^2} \Rightarrow a^2 = p \cdot b^2$. p compare un numero pari di volte in a^2, ma in numero dispari di volte in $p \cdot b^2$ quindi per il TFA ([Algebra 1 - Moci > ^1c1220]), non possono essere uguali.

Teorema: Esistono infiniti numeri primi
Dimostrazione:
Supponiamo per assurdo che esistano soltanto m numeri primi, $p_1, p_2, \ldots, p_m$ dove $m \in \mathbb{N}$.
Consideriamo $n = p_1 \cdot \ldots \cdot p_m + 1$ con $n \equiv 1(p_1), \ldots, n \equiv 1(p_m)$, quindi non è divisibile per nessuno dei primi, quindi $n \nmid p_1, \ldots, n \nmid p_m$, quindi n è irriducibile, quindi primo.

Piccolo Teorema di Fermat: Siano $a \in \mathbb{Z}, p$ primo. Allora $a^p \equiv a(p)$ ^ed2528
Dimostrazione:
Se $p|a$, stiamo dicendo che $0 \equiv 0(p)$
Se $p \nmid a$, consideriamo in $\mathbb{Z}_{/p}$ le classi dei primi $(p-1)$ multipli di a: $[a], [2a], \ldots, [(p-1)a]$
Esse sono a 2 a 2 distinte. Infatti se per assurdo $\exists 0 \leq i \neq j < p$ t.c. $[ia] = [ja]$, allora avrei che $[i] = [i][a][a^{-1}] = [j][a][a^{-1}] = [j]$, ma $i \neq j$ tra 0 e $p-1$, quindi è assurdo.
Quindi $[a], [2a], \ldots, [(p-1)a]$ sono tutti invertibili in $\mathbb{Z}_{/p}$ cioè come insieme $\{[a]; [2a]; \ldots; [(p-1)a]\} = \{1; 2; \ldots; p-1\}$ (sono uguali insiemisticamente).
Facendo i prodotti si ottiene che: $[a] \cdot [2a] \cdot \ldots \cdot [(p-1)a] = [1] \cdot [2] \cdot \ldots \cdot [p-1]$, ma nella prima parte si può raccogliere $[a^{p-1}]$, quindi $[a^{p-1}] \cdot [1] \cdot [2] \cdot \ldots \cdot [p-1] = [1] \cdot [2] \cdot \ldots \cdot [p-1]$, per quanto dimostrato prima, è possibile moltiplicare per gli inversi di $[1] \cdot [2] \cdot \ldots \cdot [p-1]$, quindi diventa $[a^{p-1}] = [1]$, moltiplicando poi per $[a]$ si ottiene $[a^p] = [a] = a^p \equiv a(p)$

Corollario: In $\mathbb{Z}_{/p}$ l'inverso di $[a](a \in \mathbb{Z}, p \neg | a)$ è $[a^{p-2}]$
Dimostrazione:
$[a] = [a^{p-2}] = [a^{p-1}] = [1]$ per la dimostrazione appena vista
Esempio:
L'inverso di $[5] \in \mathbb{Z}_{/29}$ è $[5^{27}] = [6]$

Teorema cinese del resto (veniva usato per i problemi di astronomia): Siano m, n due interi *coprimi* ($\mathcal{MCD} = 1$).
Allora l'applicazione $c: \begin{matrix} \mathbb{Z}/_{m \times n} \to \mathbb{Z}/_m \times \mathbb{Z}/_n \\ [a]_m \times n \mapsto [a]_m \times [a]_n \end{matrix}$, $\forall a \in \mathbb{Z}$ è ben definita e biunivoca.

Esempio:
$m = 2$, $n = 3$, $\mathcal{MCD} = 1$
$\mathbb{Z}/_{m \cdot n} \to \mathbb{Z}/_m \times \mathbb{Z}/_n$
$[0] \quad \mapsto ([0]; \quad [0])$
$[1] \quad \mapsto ([1]; \quad [1])$
$[2] \quad \mapsto ([0]; \quad [2])$
$[3] \quad \mapsto ([1]; \quad [0])$
$[4] \quad \mapsto ([0]; \quad [1])$
$[5] \quad \mapsto ([1]; \quad [2])$
Ogni coppia di numero compare una volta soltanto

Controesempio:
$m = 4$, $n = 6$, $\mathcal{MCD} = 2$
c non è suriettiva: $([0]_4; [1]_6) \notin Im(c)$, un numero non può essere né pari né dispari
c non è neanche iniettiva: $c([0]_{24}) = ([0]; [0]) = c([12]_{24})$, ma $c([0]_{24}) \neq c([12]_{24})$

Dimostrazione:
c è ben definita perché se $[a]_{n \cdot m} = [a']_{n \cdot m} = m \cdot n | a - a' \Rightarrow m | a - a'$ e $n | a - a' \Rightarrow [a]_m = [a]_n$ e $[a']_m = [a']_n$. c è iniettiva perché $c([a]_{mn}) = c([a']_{mn}) \Rightarrow ([a]_m; [a]_n) = ([a']_m; [a']_n) \Rightarrow m | a - a'$ e $n | a - a'$. Visto che $\mathcal{MCD} = 1$ sono coprimi, quindi $m \cdot n | a - a' \Rightarrow [a]_{mn} = [a']_{mn}$. Quindi è iniettiva, ma $|\mathbb{Z}/_{mn}| = m \cdot n = |\mathbb{Z}_m| \cdot |\mathbb{Z}_n|$, ciò implica che è anche suriettiva (di conseguenza è biettiva).

Definizione di Funzione ϕ di Eulero: Si definisce la funzione ϕ, una funzione che $\forall n \in \mathbb{N}, n \geq 2$, la funziona che associa ad ogni numero il numero degli invertibili in $\mathbb{Z}/_n$ (oppure che i numeri coprimi $0 \leq k < n$)

Esempio:
$\phi(6) = 2;\ \phi(5) = 4$ più in generale $\phi(p) = p - 1$

Proposizione:

1. Se p è primo e $r \in \mathbb{N}, r > 0$, allora $\phi(p^r) = p^r - p^{r-1}$
2. Se $m, n \in \mathbb{Z}$ t.c. $\mathcal{MCD} = 1$ allora $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$
   Dimostrazione:
   1. Siano i numeri $1, 2, \ldots, p, p+1, \ldots, 2p, \ldots, p^2$. Tra questi i numeri non coprimi con p sono i soli multipli di p. Quindi i numeri coprimi sono $\frac{p^r}{p} = p^{r-1}$
   2. Lo si dimostrare attraverso la cardinalità degli insiemi: $\{([b]_m; [c]_n) \in \mathbb{Z}/_m \times \mathbb{Z}/_n | [b]_m \text{ è invertibile e } [c]_n \text{ è invertibile}\}$, ma per il teorema cinese del resto, sono invertibili in $\mathbb{Z}/_{mn}$: $\{[a]_{mn} \in \mathbb{Z}_{mn} \mid [a]_{mn} \text{ sia invertibile}\}$. Poiché il fatto che a non abbia divisori in comune né con m né con n equivale al fatto che non abbia divisori in comune con mn

Osservazione: Questa proposizione ci permette di calcolare la funzione di Eulero $\phi(n)$ per qualsiasi n, fattorizzandolo.

Esempio:
$\phi(360) = \phi(5 \cdot 72) = \phi(5 \cdot 3^2 \cdot 2^3) = \phi(5) \cdot \phi(3^2) \cdot \phi(2^3) = (5^1 - 5^0) \cdot (3^2 - 3^1) \cdot (2^3 - 2^2) = 96$

Teorema di Eulero: Siano $a, n \in \mathbb{Z}$ t.c. $\mathcal{MCD}(a, n) = 1$, allora $a^{\phi(n)} \equiv 1\ (n)$

Esempio:
$77^{96} \equiv 1\ (360)$

Osservazione: Quando n è primo, il teorema di Eulero dice che $a^{n-1} \equiv 1\ (n)$, cioè il Piccolo Teorema di Fermat (Algebra 1 - Moci > ^ed2528) $\forall a$ t.c. $n \neg| a$. Cioè il teorema di Eulero generalizza il Piccolo Teorema di Fermat
Dimostrazione (molto simile a quella del piccolo teorema di Fermat):
Consideriamo l'insieme delle classi invertibili $\{[b_1]; [b_2]; \ldots; [b_{\phi(n)}]\} = U_n$. Supponiamo che se $[a]$ è invertibile, la moltiplicazione per $[a]$ da una biezione di U_n con se stesso:
$U_n = \{[b_1]; [b_2]; \ldots; [b_{\phi(n)}]\} = \{[a] \cdot [b_1]; [a] \cdot [b_2]; \ldots; [a] \cdot [b_{\phi(n)}]\}$. Moltiplicando per gli inversi di $[b_1]; [b_2]; \ldots; [b_{\phi(n)}]$ si ottiene: $[1] = [a^{\phi(n)}] \Rightarrow a^{\phi(n)} = 1$.

Equazioni Lineari in $\mathbb{Z}/_n$
Rappresentano tutte le equazioni del tipo $[a] \cdot [x] = [b]$ dove $[a], [b], [x] \in \mathbb{Z}/_n$. Tuttavia non si possono risolvere come le equazioni normali (nel senso di "non si possono fare tutte le cose normalmente").
Intanto possono essere viste come "congruenze lineari": $a \cdot x \equiv b\ (n)$

Proposizioni: Siano $a, b \in \mathbb{Z}$, sia $n > 1$ e sia $d = \mathcal{MCD}(a, n)$:

1. Se $d \neg| b$, la congruenza $a \cdot x \equiv b\ (n)$ non ha soluzioni;
2. Se $d | b$, $a \cdot x \equiv b\ (n)$ è equivalente alla congruenza $\frac{a}{d} \cdot x \equiv \frac{b}{d}\ (\frac{n}{d})$
3. Se $d = 1$ allora la soluzione è un'unica classe in $\bmod n$

Esempio:
$6x \equiv 5\ (9), \quad \mathcal{MCD}(6, 9) = 3, \quad 3 \neg| 5,$ quindi non ammette soluzioni
$6x \equiv 6\ (9), \quad \mathcal{MCD}(6, 9) = 3, \quad 3 | 6 \Rightarrow 2x \equiv 2\ (3),$ visto che 2 è invertibile in $\mathbb{Z}/_3 \Rightarrow x \equiv 1\ (3) \Leftrightarrow x \equiv 1, 4, 7\ (9)$

Dimostrazione:
Se x è una soluzione di $a \cdot x \equiv b\ (n)$
1. Allora $\exists k \in \mathbb{Z}$ t.c. $b = a \cdot x + k \cdot n$ e quindi (poiché $d | a$ e $d | n$) $d | b$
2. Supponiamo $d | b$. È chiaro che $a \cdot x \equiv b\ (n)$ è multiplo di n se e solo se $\frac{a}{d} \cdot x - \frac{b}{d}$ è divisibile per $\frac{n}{d}$
3. In questo caso, $[a] \in \mathbb{Z}/_n$ è invertibile, quindi basta moltiplicare per il suo inverso $[c] = [a^{-1}]$. Quindi la soluzione diventa: $[a][x] = [b]\ (n) \Leftrightarrow [x] = [b][c]\ (n) \Rightarrow x \equiv b \cdot c\ (n)$

Poi ci possono essere casi in cui i risultati non possono essere unici, come in $3x \equiv 0\ (3)$

Esempi di Sistemi di Congruenze Lineari:

$\begin{cases} x \equiv 4\ (6) \\ x \equiv 9\ (15) \end{cases}$ Per il Teorema Cinese del Resto Algebra 1 - Moci > ^66a041, si ha che è equivalente a: $\begin{cases} x \equiv 0\ (2) \\ x \equiv 1\ (3) \\ x \equiv 0\ (3) \\ x \equiv 4\ (5) \end{cases}$ ma si può vedere chiaramente che il sistema è impossibile in quanto non esiste numero che possa essere congruo a due numeri contemporaneamente in modulo 3.

$\begin{cases} x \equiv 4\ (6) \\ x \equiv 10\ (15) \end{cases}$ Per il Teorema Cinese del Resto $\begin{cases} x \equiv 4\ (6) \\ x \equiv 10\ (15) \end{cases} = \begin{cases} x \equiv 0\ (2) \\ x \equiv 1\ (3) \\ x \equiv 1\ (3) \\ x \equiv 0\ (5) \end{cases}$ *(volendo qua si potrebbe rimuovere una delle due congruenze in* $\bmod 3$ *in quanto dammo lo stesso risultato)*. Risolvere queste tre congruenze, sempre per il Teorema Cinese del Resto equivale a risolvere un uguaglianza in modulo $2 \cdot 3 \cdot 5 = 30$. In questo caso bisogna trovare un numero multiplo di 10 e $x \equiv 1\ (3)$; 10 è il caso nostro.

Esempio:
Risolvere il seguente sistema:
$\begin{cases} x \equiv 25\ (56) \\ x \equiv 7\ (45) \end{cases}$. Poiché 45 e 56 sono coprimi, la soluzione esiste per il teorema cinese del resto e la soluzione è unica (in modulo $45 \cdot 56$). Basta trovare l'identità di Bézout tra 45 e 56: $1 = 5 \cdot 45 - 4 \cdot 56$
A questo punto è sufficiente prendere $x = 25 \cdot 5 \cdot 45 - 7 \cdot 4 \cdot 56$, infatti se sostituiamo in modulo 56 si ottiene la seconda congruenza, mentre se sostituiamo in modulo 45 si ottiene la prima congruenza.
A questo punto basta risolvere $x = 25 \cdot 5 \cdot 45 - 7 \cdot 4 \cdot 56$ e si ritrova la soluzione in modulo $45 \cdot 56$

Crittografia

Crittografia: Tecniche per la decodifica di un messaggio

Definizione di Numeri Liberi da Quadrati: Un intero $n \geq 2$ è libero da quadrati se nessun primo della sua fattorizzazione compare con esponente maggiore di 1, cioè $n = p_1 \cdot \ldots \cdot p_\ell$ con $\ell > 1$ e $p_i \neq p_j, \forall i, j$.

Proposizione: Sia $n \in \mathbb{N}$ un numero libero da quadrati. Allora $\forall a, k \in \mathbb{Z}, k > 0$ si ha che $a^{k\phi(n)+1} \equiv a\ (n)$
Osservazione: Se n è primo allora è il piccolo teorema di Fermat
Dimostrazione:
Sia $i \in \{1, \ldots, \ell\}$. Se $p_i \nmid a$, allora per il Piccolo Teorema di Fermat, $a^{p_1 - 1} \equiv 1\ (p_i)$ e dunque poiché $\phi(n) = (p_1 - 1) \cdot \ldots \cdot (p_\ell - 1) \Rightarrow (p_i - 1) | k\phi(n)\ \forall k \in \mathbb{Z} \Rightarrow a^{k\phi(n)} \equiv 1\ (p_i) \Rightarrow a^{k\phi(n)+1} \equiv a\ (p_i)$. Se $p_i | a \Rightarrow 0 \equiv 0$, quindi $a^{k\phi(n)+1} \equiv a\ (p_i)$. Poiché in entrambi i casi si ha che $a^{k\phi(n)+1} \equiv a\ (p_i)\ \forall i \in 1, \ldots, \ell$, allora la cosa è valida anche per il loro prodotto: $n = p_1 \cdot \ldots \cdot p_\ell \Rightarrow a^{k\phi(n)+1} \equiv a\ (n)$

Osservazione Preliminare: Posso esprimere ogni messaggio in forma di numero
Esempio:
$0, 1, \ldots, 9, A \to 10, B \to 11, \ldots, Z \to 35, \text{spazio} \to 16, ? \to 37$

Primo Metodo: Andrea e Barbara, che vogliono mandarsi messaggi, scrivono una classe $[c]$ invertibile in $\mathbb{Z}/_{37}$ e poi moltiplicare tutti i numeri per questa classe. Quando Andrea manda il messaggio a Barbara, moltiplica ciascun numero per $[c]$ e Barbara, per decifrarlo, moltiplicano per l'inverso di $[c]^{-1}$.
Esempio:
$[c] = [2]$ e $[c]^{-1} = [19] \Rightarrow [2][19] = [38] = [1]$
Difetti:

1. Facile scoprire decifrare il messaggio (basta fare n tentativi, nel nostro esempio 37)
2. Bisogna che Andrea e Barbara i siano scambiati le chiavi in precedenza

Secondo Metodo:
Vantaggi:

1. Sicuro
2. Chiave pubblica che conoscono tutti e che non occorre scambiarsi in precedenza, che permette di scrivere messaggi, poi c'è una chiave privata che serve solo per chi deve leggerli
   Funzionamento: Barbara sceglie un numero $n \in \mathbb{N}$ libero da quadrati ed $e \in \mathbb{N}$ coprimo $\phi(n)$. Barbara comunica a tutti la chiave pubblica che è fatta dalla coppia (n, e), ma Barbara è l'unica a conoscere la fattorizzazione di n e

quindi a conoscere $\phi(n)$. Andrea vuole trasmettere a Barbara un messaggio M. Assumiamo che $M \in \mathbb{N}$ e supponiamo $M < n$ (altrimenti lo dovremmo spezzare in messaggi più piccoli). Andrea allora eleva M all'esponente e, poi lo riduce a modulo n, ottenendo così $M' \equiv M^e\ (n)'$ con $M' < n$. Poi manda M' a Barbara. Barbara riceve M' e, poiché conosce $\phi(n)$ sa calcolare l'inverso di $[e]$ in $\mathbb{Z}/_{\phi(n)}$, cioè sa trovare $c \in \mathbb{Z}$ t.c. $ce \equiv 1\ (\phi(n))$ cioè $\exists k \in \mathbb{Z}$ t.c. $ce = k\phi(n) + 1$. Dunque Barbara eleva M' all'esponente c e poi lo riduce a a modulo n: $(M')^c \equiv (M^e)^c = M^{ec} = M^{k\phi(n)+1}$, che, per quanto detto prima è congruente a M in modulo n. Ossia ritrova il messaggio originale.

Come fa però ad essere sicura che sia proprio di Francesco? Con la Firma Digitale
Barbara ha la sua chiave (n, e) e anche Andrea ha la sua chiave (n_A, e_A), con n_A libero da quadrati, e_A coprimo con $\phi(n_A)$. Tutti conoscono (n_A, e_A) ma solo Andrea conosce $\phi(n_A)$ e quindi riesce a calcolare e_A t.c. $c_a e_A = 1$. Questo serve non solo a Barbara per rispondere ad Andrea ma anche ad Andrea per firmare digitalmente il proprio messaggio. Andrea prende la propria firma F, la eleva a c_A e la riduce a $F' \equiv F^{c_A}\ (n_a)$. Trasmette quindi la firma F' a Barbara insieme al messaggio M'. Barbara eleva quindi $(F')^{e_A}$ e ritrova la firma di Andrea $F \equiv (F')^e$

Esempio:
Siano $n = 9367\ (19 \cdot 17 \cdot 29) \quad e = 5$ Chiave di Barbara, $n_A = 1147\ (31 \cdot 37) \quad e_A = 41$ chiave di Andrea
Andrea può calcolare $\phi(n_A) = 30 \cdot 36 = 1080$ e usando l'identità di Bézout (e l'algoritmo di Euclide) si ottiene $1 = 3 \cdot 1080 - 79 \cdot 41$, da cui si ricava che $c_A = 1001$
Allo stesso modo si ricava che $\phi(n) = 8064$ e che $c = 1613$
Andrea vuole mandare il messaggio $M = 134257$ e lo firma con $F = 11$
Poiché si ha che $M > n$ si deve dividere il numero in due parti: $M_1 = 134$ e $M_2 = 257$, quindi:
$M_1' = (147)^5 \equiv 8570\ (9367); \quad M_2' = (257)^5 \equiv 3993\ (9367); \quad F' = 11^{1001} \equiv 582\ (1147)$
Quindi per decifrare i messaggi, Barbara deve fare:
$M_1 = (8570)^{1613} \equiv 134\ (9367); \quad M_2 = (3993)^{1613} \equiv 257\ (9367); \quad F = 582^{41} \equiv 11\ (1147)$

Teoria Dei Gruppi

Definizione di Gruppo: Un gruppo $(G, \star)$ è un insieme G unito da un'operazione binaria (un'applicazione $\star : G \times G \to G\ (g_1, g_2) \mapsto g_1 \star g_2$), con le seguenti proprietà:

1. $\star$ è associativa, cioè $(g_1 \star g_2) \star g_3 = g_1 \star (g_2 \star g_3)$
2. Esiste un elemento neutro e tale che $e \star g = g \star e = g$
3. Per ogni g esiste un inverso $\tilde{g}$ tale che $g \star \tilde{g} = e$
   Diciamo che $(G, \star)$ è un gruppo commutativo (o abeliano) se vale
4. $g_1 \star g_2 = g_2 \star g_1\ \forall g_1, g_2 \in G$

Esempi:
1. $(\mathbb{Z}, +)$ oppure $(\mathbb{Q}, +)$ oppure $(\mathbb{R}, +)$ oppure $(\mathbb{C}, +)$ sono dei gruppi commutativi, con l'elemento neutro 0 e l'inverso $\tilde{x} = -x$ (l'opposto)
2. $(\mathbb{N}, +)$ non è un gruppo in quanto la proprietà 3 è falsa (non c'è un inverso), $(\mathbb{N}, -)$ non è un gruppo in quanto la proprietà 1 è falsa ($(a - b) - c \neq a - (b - c)$)
3. $(\mathbb{R}, \cdot)$ non è un gruppo in quanto 0 non ha un inverso. Dato un campo $\mathbb{K}$, denotiamo con $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$. $(\mathbb{Q}^*, \cdot)$ oppure $(\mathbb{R}^*, \cdot)$ oppure $(\mathbb{C}^*, \cdot)$ sono dei gruppi commutativi con l'elemento neutro 1 e inverso $\tilde{x} = x^{-1}$
4. Più in generale un campo $(\mathbb{K}, +, \cdot)$ è un insieme con due operazioni tali che $(\mathbb{K}, +)$ e $(\mathbb{K}^*, \cdot)$ sono gruppi commutativi e vale la legge distributiva (che lega le due operazioni)
5. Dato un insieme X:
5.1. $(\mathcal{P}(X), \cup)$ non rappresenta un gruppo perché non è valida la terza proprietà
5.2. $(\mathcal{P}(X), \cap)$ non rappresenta un gruppo perché non è valida la terza proprietà
5.3. $(\mathcal{P}(X), \setminus)$ non è un gruppo perché non è valida la prima proprietà
6. Per ogni $n \in \mathbb{N}, n > 1, (\mathbb{Z}_{/n}, +)$ è un gruppo commutativo con elemento neutro $e = [0]$ e inverso $\tilde{[a]} = [a]^{-1}$
6.1. Sia $\mathbb{Z}_{/3} = \{[0], [1], [2]\}$

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

7. Per ogni $n \in N, n > 1,\ \bigcup_n = \{\text{ invertibili in } \mathbb{Z}_{/n}\}$ dove $|\bigcup_n| = \phi(n)$. $(\bigcup_n, \cdot)$ è un gruppo commutativo con elemento

neutro $[1]$
7.1. $\bigcup_8=\{[1],[3],[5],[7]\}$ e $\phi(8)=4$

$\cdot$	$[1]$	$[3]$	$[5]$	$[7]$
$[1]$	$[1]$	$[3]$	$[5]$	$[7]$
$[3]$	$[3]$	$[1]$	$[7]$	$[5]$
$[5]$	$[5]$	$[7]$	$[1]$	$[3]$
$[7]$	$[7]$	$[5]$	$[3]$	$[1]$

8. Dato uno spazio vettoriale V, $GL(V)=\{\text{ applicazioni lineari e invertibili } V\to V\}$ *(Geometria 1A - Migliorini > ^f462a4)* $(GL(V),\circ)$ è un gruppo con elemento neutro la funzione identità: $id:V\to V, v\mapsto v$ e con una funzione inversa $\tilde{g}=g^{-1}$. Però non è commutativa
8.1. $V=\mathbb{R}^2$. Siano $g\binom{x}{y}=\binom{y}{x}$ e $h\binom{x}{y}=\binom{2x}{y}$. $\begin{cases} g\circ h\binom{x}{y}=g(h\binom{x}{y})=g\binom{2x}{y}=\binom{y}{2x} \\ h\circ g\binom{x}{y}=h(g\binom{x}{y})=h\binom{y}{x}=\binom{2y}{x}\end{cases}\Rightarrow g\circ h\neq h\circ g$
9. Sia X un insieme. $Sym(X)=\{\text{ biezione di } g:X\to X\}$ è costituito da $x!$ elementi. Si ha che $(Sym(X),\circ)$ è un gruppo non commutativo
9.1. Sia $X=\{1,2,3\}$, allora $\mathfrak{S}_3=Sym\{1,2,3\}$. Si ha che $e=id$ e $\tilde{g}=g^{-1}$
Per semplicità di scriverlo, $id=id, s_1=(1,2), s_2=(2,3), t=(1,3), c=(1,2,3), c^{-1}=(1,3,2)$
Si può vedere quindi che non è simmetrica, basta fare $(S_1\circ S_2)$ e $(S_2\circ S_1)$. Infatti:
$(\mathfrak{S}_1\circ\mathfrak{S}_2)(1)=2 \qquad (\mathfrak{S}_2\circ\mathfrak{S}_1)(1)=3$
$(\mathfrak{S}_1\circ\mathfrak{S}_2)(2)=3 \qquad (\mathfrak{S}_2\circ\mathfrak{S}_1)(2)=1$
$\underbrace{(\mathfrak{S}_1\circ\mathfrak{S}_2)(3)=1}_{C} \qquad \underbrace{(\mathfrak{S}_2\circ\mathfrak{S}_1)(3)=1}_{C^{-1}}$

Definizione di Sottogruppo: Sia $(G,\star)$ un gruppo e sia H un sottoinsieme di G ($H\subseteq G$). Diciamo che H è un sottogruppo di G (scriviamo $H\leq G$) se H è esso stesso un gruppo all'operazione di G. Cioè

1. H è chiuso rispetto all'operazione $\star$: $\forall h_1,h_2\in H, h_1\star h_2\in H, h_2\star h_1\in H$
2. $e\in H$, ossia contiene l'elemento neutro;
3. $\forall h\in H, \exists\tilde{h}\in H$, ossia contiene ogni inverso

Esempi:
1. SIa $(\mathbb{Z},+)$. $H_1=\{\text{ tutti i numeri pari }\}=\{2n, n\in\mathbb{Z}\}$ rappresenta un sotto gruppo di $\mathbb{Z}$ rispetto alla somma, $H_2=\{\text{ tutti i numeri dispari}\}=\{2n+1, n\in N\}$ invece non lo è
2. Sia $(\mathbb{R}^*,\cdot)$. $H_1=]0,+\infty[$ è un sottogruppo di $\mathbb{R}^*$ perché sono vere tutte le proprietà, invece $H_2=]-\infty,0[$ non lo è
3. Sia V uno spazio vettoriale, $GL(V)$ è sottospazio di $Sym(V)$
4. Sia $\mathcal{S}_3$ dell'esempio 9.1 di prima. $H_1=\{id, S_1\}$ rappresenta un sottogruppo, mentre $H_2\{id, C\}$ no

Definizione di Omomorfismo: Siano $(G,*)$ e $(H,\star)$ due gruppi. Un'applicazione $f:G\to H$ è un omomorfismo di gruppi se $\forall g_1,g_2\in G,\ f(g_1*g_2)=f(g_1)\star f(g_2)$, cioè è la stessa cosa fare prima l'operazione di G e poi f e fare f e poi l'operazione di H

Esempio:
1. Siano $(G,*)=(\mathbb{R},+)$ e $(H,\star)=(\mathbb{R},\cdot)$. Sia data la funzione $f:\mathbb{R}\to\mathbb{R}^*,\ f(x)=e^x$. Si ottiene che $e^{x_1+x_2}=f(x_1+x_2)=f(x_1)+f(x_2)=e^{x_1}\cdot e^{x_2}$. Quindi si ha che f è un omomorfismo tra questi gruppi
2. $f:\mathbb{Z}\to\mathbb{Z}_{/n},\ f(a)=[a]$. È un omomorfismo tra $(\mathbb{Z},+)$ e $(\mathbb{Z}_{/n},+)$, $[a+b]=[a]+[b]$

Osservazione: Uno spazio vettoriale V (su un campo $\mathbb{K}$) è un gruppo commutativo $(V,+)$ con un'operazione aggiuntiva $\cdot:\mathbb{K}\times V\to V$ che verifica certe proprietà. Un sottospazio vettoriale è uno spazio vettoriale di $(V,+)$ rispetto a $\cdot$.
Un'applicazione lineare $f:V\to U$ è un omomorfismo di gruppi $(V,+)$ e $(U,+)$ compatibile anche con $\cdot$ cioè $f(\alpha v)=\alpha f(v)$

Proposizione: L'elemento neutro è unico
Dimostrazione:
Supponiamo che esistono due elementi neutri $e,u\in G$ con la proprietà che $e\star g=g=g\star e$ e $u\star g=g=g\star u,\forall g\in G$.
Si ottiene he $e=e\star u=u$, quindi $e=u$
In modo simile può dimostrare che l'inverso è unico.

Definizione: Sia $(G,\star)$ un gruppo e $g\in G$ e definiamo Ordine (o Periodo) di G come il minimo n, con $n\geq 1$, t.c. $\underbrace{g\star g\star g\star\ldots\star g}_{n \text{ volte}}=e$. Si scrive $o(g)=n$ oppure $o(g)=\infty$ se non esiste.

Esempio:
1. $(\mathbb{Z},+)$ con $e=0$. Si ha che $o(0)=1$ e $o(1)=\infty$
2. $(\mathbb{Z}_{/6},+)$ con $e=[0]$. Si ha che $o([0])=1$, $o([1])=6$, $o([2])=3$
3. $(\mathbb{R}^*,\cdot)$ con $e=1$. Si ha che $o(1)=1$, $o(-1)=1$ e $o(\text{qualsiasi altro numero})=\infty$
4. $(\mathfrak{S}_3,\circ)$ (Per riprendere sopra) $o(s_1)=2$ e $o(c)=3$

Osservazione: Sia $(\mathbb{K},+,\cdot)$ un campo. La caratteristica di $\mathbb{K}$ è l'ordine di 1 (elemento neutro della seconda operazione) in $(\mathbb{K},+)$. Convenzionalmente si dice che è a caratteristica 0 o "non infinita".

Definizione di Nucleo e Immagine: Dato un omomorfismo $f:G\to H$, definiamo $Ker(f)=\{g\in G\mid f(g)=e_H\}$ e $Im(f)=\{f(g)\in G\}=\{h\in H\mid \exists g\in G \text{ t.c. } f(g)=h\}$

Osservazione: $Ker(f)\leq G$ e $Im(f)\leq H$. f iniettiva $\Leftrightarrow Ker(f)=\{e\}$ e f suriettiva $\Leftrightarrow Im(f)=H$

Esempio:
$(\mathbb{Z},+)$ e $(\mathbb{C}^*,\cdot)$. Data la funzione $f:\begin{matrix}\mathbb{Z}\to\mathbb{C}^*\\ n\mapsto i^n\end{matrix}$, si ha che la funzione non è suriettiva: $Im(f)=\{1,i,-1,-i\}$. Questo è un sottogruppo per omomorfismo in f. Infatti $f(m+n)=i^{m+n}=i^m+i^n=f(m)\cdot f(n)$ e
$Ker(f)=\{4n,n\in\mathbb{Z}\}=\{m\in\mathbb{Z} \text{ t.c. } m\equiv 0\}=4\mathbb{Z}$

Definizione: Un'applicazione $f:G\to H$ è un "isomorfismo di gruppo" se è un omomorfismo di gruppi ed è biunivoca ^48fd47
Diciamo che 2 gruppi $(G,\star)$ e $(H,*)$ sono isomorfi se esiste un isomorfismo $G\to H$

Osservazione: È una relazione di equivalenza (Infatti $R=$ la funzione identità, $S=$ funzione inversa, $T=$ composione di funzioni)

Osservazione: Dato un gruppo $(G,\star)$, definiamo l'insieme degli Automorfismi. $Aut=\{\text{ Isomorfismi } G\to G\}$ e $(Aut(G),\circ)$ è un gruppo, o meglio, un sottogruppo di $Sym(G)$

Esempio:
$\varphi:\begin{matrix}\mathbb{Z}_{/n}\to\{1,i,-1,-i\}\\ [n]\mapsto i^n\end{matrix}$ è ben definita, iniettiva, suriettiva e c'è un omomorfismo. Quindi φ è un isomorfismo di gruppi, ossia il funzionamento è lo stesso.

Osservazione: I due gruppi hanno la stessa struttura, cioè funzionano allo stesso modo

Esempio:
$f:\mathbb{R}\to]0;+\infty[\quad f(x)=e^x$. È un omomorfismo $e^{x_1+x_2}=e^{x_1}\cdot e^{x_2}$
Questa funzione è biunivoca, infatti l'isomorfismo inverso è $f^{-1}]0;+\infty[\to\mathbb{R}$ è $f^{-1}(y)=x$

Sia $n\in N, n\geq 2$. Nel piano cartesiano $\mathbb{R}^2$ indichiamo con r la rotazione di centro l'origine e angolo $\frac{2\pi}{r}$. Indichiamo con $r^k=\underbrace{r\circ\ldots\circ r}_{k\text{ volte}}$
Osservazione: $R_n=\{id,r,r^2,\ldots,r^{n-1}\}$ è un gruppo rispetto alla composizione (l'elemento neutro e è $r^n=id$ e l'inverso di r^k è r^{n-k})

Esempio:
Se $n=12$, r= rotazione di 30° $R_{12}=\{r,r^2,\ldots,r^{11},r^{12}=id\}$
Osservazione: R_{12} rispetto alla composizione è isomorfo a $\mathbb{Z}_{/12}$. È anche isomorfo a all'orologio: $\begin{matrix}\mathbb{Z}_{/12}\to R_{12}\\ [k]\mapsto r^k\end{matrix}$
Nello specifico l'isomorfimo è ben definito, iniettivo, suriettivo e omomorfo
Analogamente $\mathbb{Z}_{/n}$ è isomorfo a $(R_n,\circ)$

Osservazione: $(R_4,\circ)$ e $\mathbb{Z}_{/4}$ sono isomorfi a $\overbrace{\{1,i,-1,-i\}}^{C_4}$ rispetto al prodotto

Esempio:
Considero il gruppo $\mathbb{Z}^2_{/2}$ rispetto alla somma per cardinalità: $\mathbb{Z}^2_{/2}=\{\underbrace{([0],[0])}_{e},\underbrace{([1],[0])}_{\text{Ordine}=2},\underbrace{([0],[1])}_{\text{Ordine}=2},\underbrace{([1],[1])}_{\text{Ordine}=2}\}\}$
Questo insieme ha 4 elementi, volendo potrei metterlo in relazione con gli altri, ma non è isomorfo con quelli precedenti.
Supponiamo che esista un isomorfismo $f:\mathbb{Z}^2_{/2}\to\mathbb{Z}_4$ e sia x l'elemento $\in\mathbb{Z}^2_{/2}$ tale che $f(x)=[1]\in\mathbb{Z}_4$
Allora per l'isomorfismo si ha che $f(x+x)=([0],[0])$ ma la cosa è impossibile in quanto
$[2]=[1]+[1]=f(x+x)\neq f([0],[0])=[0]$, quindi non è un isomorfismo.

Esempio:
Consideriamo le trasformazioni del piano fissato un rettangolo di centro l'origine degli assi (ossia l'intersezione degli assi) e siano le funzioni $g(x,y)=(-x,y)$; $g(x,y)=(x,-y)$ e $g\circ h(x,y)=(-x,-y)$ (ossia ribaltamenti)
In particolare g è la simmetria rispetto all'asse x, h è la simmetria rispetto all'asse y e $g\circ h$ è la rotazione di 180°
Questo particolare gruppo $K_4=\{id,g,h,g\circ h\}$ con $\circ$ si chiama "Gruppo di Klein" (o della carta di credito)
Osservazione: è isomorfo a $\mathbb{Z}^2_{/2}$, infatti: $id=[0],[0]$, $g=[1],[0]$, $h=[0],[1]$ e $g\circ h=[1],[1]$

Esempio:
Considero $(\mathbb{Z},+)$ e $(\mathfrak{S}_3,\circ)$. Sono isomorfi? No, Questo è già osservabile dal fatto che il primo è commutativo, il secondo no

Osservazione: L'intersezione di sottogruppi è un sottogruppo
Dimostrazione: Sia G un gruppo e siano $\{G_i,\ i\in I\}$ un insieme dei suoi sottogruppi. Mostriamo che $H=\bigcap_{i\in I}G_i$ è un sottogruppo di G. Siano $g_1,g_2\in H\Rightarrow g_1,g_2\in G_i\ \forall i\in I$. Poiché $G_i\leq G\Rightarrow g_1\star g_2\in G_i\ \forall i\in I\Rightarrow g_1\star g_2\in H=\bigcap_{i\in I}G_i$.
Analogamente si dimostra per l'elemento neutro e gli inversi (e appartiene in tutti $\Rightarrow e\in H$, idem per $\tilde{g}\in H$)

Osservazione: L'unione di tutti i sottogruppi non è un sottogruppo. (Stessa dimostrazione di geometria)

Definizione di Sottogruppo Generato: Sia $(G,\star)$ un gruppo e sia $X\subseteq G$ (quindi un sottoinsieme). Definiamo il sottogruppo generato da X, indicato con $\langle X\rangle$, come il più piccolo sottogruppo di G che contiene X, ovvero l'intersezione di tutti i sottogruppi di G che contengono X. Concretamente
$\langle X\rangle=\{g_1\star g_2\star\ldots\star g_\ell \text{ dove } g_i\in X\wedge\tilde{g}_i\in X,\ \forall i\in\mathbb{N},\ \ell>0\}$

Esempi:
1. $(\mathbb{Z}^n,+)$, il suo insieme di generatori è $\langle X\rangle=\{e_1,\ldots,e_n\}$ vettori della base canonica
2. $(\mathbb{Q}^*,\circ)$, il suo sottogruppo di generatori è $\langle X\rangle=\{-1,\ \text{tutti i numeri primi}\}$. Attraverso le combinazioni lineari di questi elementi è possibile creare tutto $\mathbb{Q}^*$

Definizione di Gruppo Ciclico: Un gruppo G è ciclico se $\exists g\in G$ t.c. $\langle g\rangle=G$

Esempi:
1. $(\mathbb{Z},+)$ è un gruppo ciclico, infatti $\mathbb{Z}=\langle 1\rangle=\langle -1\rangle$
2. $(\mathbb{Z}_{/n},+)$ è un gruppo ciclico, infatti $\mathbb{Z}_{/n}=\langle[\pm1]\rangle$ (A meno di isomorfismi, non ce ne sono altri)

Proposizione: Sia $(G,\star)$ un gruppo ciclico con $G\neq\langle e\rangle$. Allora G è isomorfo a $(\mathbb{Z},+)$ oppure a $(\mathbb{Z}_{/n},+)$
Dimostrazione:
Per Ipotesi $\exists g\in G$ tale che $\langle g\rangle=G$
1. Se $o(g)=\infty$, allora posso considerare $G=\{\ldots,g^{-2},g^{-1},e,g,g^2,\ldots\}=\{g^n,n\in\mathbb{Z}\}$. Quindi $\begin{matrix}Z\to G\\ n\mapsto g^n\end{matrix}$ è biunivoca ed è omomorfismo perché $g^{n+m}=g^n\star g^m$
2. Se $o(g)=n$ con $n>1$, allora $G=\{g,g^2,\ldots,g^n=e\}$. Quindi l'applicazione $\begin{matrix}\mathbb{Z}_{/n}\to G\\ [a]\mapsto g^a\end{matrix}$ è ben posta, biunivoca ed è un omomorfismo per la stessa ragione di prima. Quindi si tratta di un isomorfismo.

Esempi:
1. $\{i,i^2=-1,i^3=-i,i^4=1\}\simeq\mathbb{Z}_{/n}=\{[0],[1],[2],[3]\}$
2. $(R_n,\circ)$ è isomorfo a $(\mathbb{Z}_{/n},+)$

Come sono fatti i sottogruppi dei gruppi ciclici?

Definizione di Multipli di Sottogruppo: Per ogni $m\in\mathbb{Z}$, definiamo con $m\mathbb{Z}$ i multipli di $\mathbb{Z}$ tale che $m\mathbb{Z}=\{ma,a\in\mathbb{Z}\}$. $m\mathbb{Z}$ è un sottogruppo di $\mathbb{Z}$ ciclico, generato da m. $m\mathbb{Z}_{/n}=\{[m][a],[a]\in\mathbb{Z}_{/n}\}$ è un sottogruppo di $\mathbb{Z}_{/n}$ generato da $[m]$.

Esempi:
1. $6\mathbb{Z}_{/12}=\langle X\rangle=\{[6],[0]\}\simeq\mathbb{Z}_{/2}$
2. $4\mathbb{Z}_{/12}=\langle X\rangle=\{[4],[8],[0]\}\simeq\mathbb{Z}_{/3}$
3. $3\mathbb{Z}_{/12}=\langle X\rangle=\{[3],[6],[9],[0]\}\simeq\mathbb{Z}_{/4}$
4. $2\mathbb{Z}_{/12}=\langle X\rangle=\{[2],[4],[6],[8],[10],[0]\}\simeq\mathbb{Z}_{/2}$
5. $5\mathbb{Z}_{/12}=\mathbb{Z}_{/12}$

Teorema:

1. Tutti i sottogruppi di $(\mathbb{Z}, +)$ sono della forma $m\mathbb{Z}$ per qualche $m \in \mathbb{Z}$
2. Tutti i sottogruppi di $(\mathbb{Z}_{/n}, +)$ sono della forma $m\mathbb{Z}_{/n}$ per qualche $m|n$.
   Dimostrazione:
   1. Sia $H \subseteq \mathbb{Z}$. Se $H = \{0\}$, basta prendere $m = 0$. Altrimenti H contiene almeno un intero strettamente positivo. Sia n in più piccolo intero positivo in H. Vogliamo mostrare che $m\mathbb{Z} = H$. Poiché H è un è un sottogruppo di $\mathbb{Z}$, sicuramente $m\mathbb{Z} \subseteq H$. D'altra parte sia $h \in H$. Facciamo la divisione per m: $h = mq + r$ con $0 \leq r < m$. Ma $r = h - mq$ e per non contraddire la minimalità di m deve essere $r = 0 \Rightarrow m|h \Rightarrow h \in m\mathbb{Z} \Rightarrow H \subseteq m\mathbb{Z}$. Unendo queste due affermazioni si ottiene che $H = m\mathbb{Z}$
   2. Sia $H \leq \mathbb{Z}_{/n}$. Se $H = \{[0]\}$, basta scegliere $m = 0$, altrimenti sia m il più piccolo intero positivo tale che $[m] \in H$. Ragionando come nel punto precedente, si vede che $H = m\mathbb{Z}_{/n}$

Proposizione: Sia $a \in \mathbb{Z}$, sia $n \geq 2$ e sia $d = \mathcal{MCD}(a, n)$. Allora,

1. L'ordine in $\mathbb{Z}_{/n}$ di $[a]$ è $\frac{n}{d}$
2. a in $\mathbb{Z}_{/n} = d$ in $\mathbb{Z}_{/n}$
   Esempio:
   $o([9]) = 4$ in $\mathbb{Z}_{/n}$ e $9\mathbb{Z}_{/n} = 3\mathbb{Z}_{/n}$
   Dimostrazione:
   1. L'ordine di $[a]$ in $\mathbb{Z}_{/n}$ è il più piccolo intero $x > 0$ tale che $ax \equiv 0\ (n)$. Per quanto visto sulle congruenze lineari, tale congruenza è equivalente a $\frac{a}{d}x \equiv 0\ (\frac{n}{d})$, la quale ha soluzione unica modulo $(\frac{n}{d})$. Quindi la più piccola soluzione positiva è $x = \frac{n}{d}$
   2. Per il punto precedente $o([a]) = \frac{n}{d} = o([d])$. Poiché a è multiplo di d, $a\mathbb{Z}_{/n} = \langle [a] \rangle \leq \langle d \rangle = d\mathbb{Z}_{/n}$. Ma poiché $o([a]) = o([d])$ devono avere la stessa cardinalità e dunque coincidono.

Definizione di Prodotto Diretto di Gruppi: Dati due gruppi $(G, *)$ e $(H, \star)$, il loro prodotto diretto è $(G \times H, \heartsuit)$. Infatti $(g_1, h_1) \heartsuit (g_2, h_2) = (g_1 * g_2, h_1 \star h_2)$

Esempio:
$\mathbb{Z}_{/n} \times \mathbb{Z}_{/m}$ con la somma coordinata per coordinata

Osservazione: Il Teorema Cinese del Resto ci dice che se $\mathcal{MCD}(m, n) = 1$, $c : \begin{matrix} \mathbb{Z}_{m,n} \to \mathbb{Z}_n \times \mathbb{Z}_m \\ [a]_{n,m} \mapsto ([a]_n, [a]_m) \end{matrix}$ è una biezione.
In effetti c è un isomorfismo: $[a]_{n,m} + [b]_{n,m} = [a + b]_{n,m} \mapsto ([a + b]_n, [a + b]_m)$

Esempio:
$\mathbb{Z}_{/12}$ è isomorfo come gruppo a $\mathbb{Z}_{/4} \times \mathbb{Z}_{/3}$

Osservazione: un elemento $[a]$ genera $\mathbb{Z}_{/n} \Leftrightarrow$ ha ordine $n \Leftrightarrow \mathcal{MCD}(a, n) = 1$. Quindi ci sono $\phi(n)$ generatori.

Esempio:
$\mathbb{Z}_{/12}$ è generato da $[1]$ ma anche da $[5], [7]$ e $[11]$ in quanto $\phi(12) = 4$

Teorema: Sia $f : G \to H$ un omomorfismo di gruppi. Allora $\forall g \in G$, l'ordine $o(f(g))|o(g)$. Inoltre se f è isomorfismo, $o(f(g)) = o(g)$
Dimostrazione:
Sia $n = o(g)$ e sia $d = o(f(g))$. Poiché $g^n = e_G$, essendo f un omomorfismo $f(g^n) = f(e_G) = e_H$, ma per omomorfismo $f(g^n) = (f(g))^n \Leftrightarrow f(g) \star f(g) \star \ldots \star f(g)$. Quindi $f \leq n$. Facciamo la divisione, $n = dq + r$ con $0 \leq r < d$. Quindi $e_H = (f(g))^n = (f(g))^{dq+r} = (\underbrace{(f(g))^d}_{e_H})^q \star (f(g))^r = e_H \star (f(g))^r$. Poiché $r < d$ e d è l'ordine, deve essere necessariamente $r = 0$, Quindi $d|n$. Se f è isomorfismo, esiste $f^{-1} : H \to G$ che è anche esso un isomorfismo. Applicando quindi la prima parte ad entrambi si ottiene $n|d$ e $d|n \Rightarrow n = d$

Osservazione: Il teorema non dice che un'applicazione che manda ciascun elemento in uno dello stesso ordine è isomorfismo. Se G è ciclico e g è un suo generatore, f è determinato dalla scelta di $f(g)$, per cui $f(g^n) = (f(g))^n$

Esempio:
Troviamo tutti gli omomorfismi $\mathbb{Z}_{/6} \to \mathbb{Z}_{/9}$ con l'operazione somma:
Si ha che $\mathbb{Z}_{/6} = \{[0], [1], [2], [3], [4], [5]\}$ e $\mathbb{Z}_{/9} = \{[0], [1], [2], [3], [4], [5], [6], [7], [8]\}$
$o(f[1]) = 1, 2, 3, 6$, in quanto ogni elemento di $\mathbb{Z}_{/6}$ può avere questo ordine. Per quanto detto sopra bisogna mandare ogni elemento di quest'ordine in uno dello stesso ordine in $\mathbb{Z}_{/9}$, quindi 2 e 6 non vanno bene (non sono ordini di

elementi di $\mathbb{Z}_{/9}$)
Quindi si può mandare $f(1) = 3, f(1) = 6, f(1) = 0$. Quindi ci sono 3 omomorfismi possibili.

Gruppi Diadrali
Definizione di Gruppo Diadrale: Sia P_n un poligono regolare di n lati, centrato nell'origine. $\mathfrak{D}_n$ rappresenta i movimenti rigidi del piano che mandando P_n in sé stesso. I suoi elementi sono
$\mathfrak{D}_n = \{\underbrace{r, r^2, \dots, r^{n-1}, r^n = id}_{\text{Rotazioni}}, \underbrace{s_1, s_2, \dots, s_n}_{\text{Simmetrie}}\}$

Esempio:
Dato un pentagono regolare, r rappresenta una rotazione di $72^\circ = \frac{2\pi}{5}$.
Quindi $\{r, r^2, r^3, r^4, r^5 = id\} \subseteq \mathfrak{D}_5$
Anche gli assi di simmetria da un vertice al punto medio del lato opposto sono elementi di $\mathfrak{D}_5$
Quindi $\mathfrak{D}_5 = \{r, r^2, \dots, r^5 = id, s_1, s_2, \dots, s_5\}$

Domanda: È un gruppo?
In generale $(\mathfrak{D}, \circ)$ è un gruppo. L'elemento neutro e è id. L'inverso di una rotazione r^k è r^{n-k}, infatti $r^k \circ r^{n-k} = r^n = id$.
L'inverso di una simmetria è se stessa.

Osservazione: In generale $(\mathfrak{D}, \circ)$ ha $2n$ elementi. Ha anche un sottogruppo, costituito dalle sole rotazioni $(= R_n)$, ma non c'è il sottogruppo delle simmetrie, in quanto la composizione di due simmetrie da una rotazione.

Come fare i conti in $\mathfrak{D}$?

Osservazione: In un gruppo, $(g \tilde{\star} h) = \tilde{h} \star \tilde{g}$, perché $g \star h \star \tilde{H} \star \tilde{g} = g \star \tilde{g} = e$
Osservazione: $r \circ s = s_2$, ma anche $r \circ s_2 = s_3$ e $r \circ s_3 = s_4$ e così via. Quindi $\mathfrak{D}$ è generato da $\{r, s\}$
Osservazione: Poiché $\forall k, r^k s$ è una simmetria, si ha che $r^k s = (r^k s)^{-1} = s^{-1}(r^k)^-1 = sr^{n-k}$. Questa relazione è utile per i conti

Esempio:
$s_2 \circ s_4 = r \circ s \circ r^3 \circ s = r \circ r^2 \circ s \circ s \circ s = r^3$

Osservazione: $\mathfrak{D}_n$ è generato anche da $\{s, rs\}$ perché posso ottenere r con $r \circ s = r$

Teorema di Cayley: Sia G un gruppo. Allora esiste un omomorfismo iniettivo $M : G \to Sym(G)$ ^4a837d
Osservazione:

1. Se $|G| = n$, numerando gli elementi di G si ha che $Sym(G) = \mathfrak{S}_n$
2. Dato un omomorfismo iniettivo $M : G \to Sym(G)$ significa trovare un sottogruppo di $Sym(G)$ isomorfo a G ($Im(M)$).
3. "Tutti i gruppi finiti sono contenuti in Sym per un n abbastanza grande"
   Dimostrazione:
   Per ogni $g \in G$, consideriamo $m_g : \begin{matrix} G \to G \\ h \mapsto g \star h \end{matrix}$. m_g è invertibile con inversa $m_{\tilde{g}}$, quindi m_g è biunivoca, ovvero $m_g \in Sym(g)$. Definisco un'applicazione $M : \begin{matrix} G \to Sym(G) \\ g \mapsto m_g \end{matrix}$. M è un omomorfismo tra $(G, \star)$ e $(Sym(G), \circ)$ perché $M(g_1 \star g_2) = m_{(g_1 \star g_2)} = m_{g_1} \circ m_{g_2} = M(g_1) \circ M(g_2)$. M è iniettiva perché se $M(g_1) = M(g_2)$, allora $M(g_1)(h) = M(g_2)(h)\ \forall h \in G$. In particolare se $h = e$, $mg_1(e) = mg_2(e) \Rightarrow g_1 = g_2 \Rightarrow M$ è iniettiva.

Exempio:
$(G, \star) = (\mathbb{Z}_{/3}, +)$. Gli elementi di $\mathbb{Z}_{/3} = \{[0], [1], [2]\}$ Sia l'applicazione: $m_{[0]} : [a] \mapsto [0] + [a] = [a]$ quindi $m_{[0]} = id$
$m_{[1]} : [a] \mapsto [1] + [a]$ si ottiene c di [Algebra 1 - Moci > ^5bb0aa]
Analogamente $m_{[2]} : [a] \mapsto [2] + [a]$ e si ottiene c^{-1} di [Algebra 1 - Moci > ^5bb0aa]

Osservazione: Spesso si può far di meglio per alcuni gruppi.
$|\mathfrak{D}_5| = 10$. Per il teorema di Cayley c'è omomorfismo iniettivo di $\mathfrak{D}_5 \to \mathfrak{S}_{10}$ ma $|\mathfrak{S}_{10}| = 10!$.
In realtà si può immergere $\mathfrak{D}_5$ in $\mathfrak{S}_5$ Sfruttando i vertici di un poligono.

Definizione di Gruppo Simmetrico: $(\mathfrak{S}_n, \circ) = Sym(\{1, \dots, n\}) = \{\text{Biezioni } \{1, \dots, n\} \to \{1, \dots, n\}\}$.

Definizione di Permutazione: Gli elementi di $\mathfrak{S}_n$ sono dette permutazioni e sono $n!$

Definizione di Orbita: Dato $i \in \{i, \dots, n\}$ e dato $\sigma \in \mathfrak{S}_n$. Definisco l'orbita di i come
$O\sigma(i) = \{i, \sigma(i), \sigma(\sigma(i)) = \sigma^2(i), \sigma(i), \dots\}$

Esempio:
Sia per esempio $\sigma \in \mathfrak{S}$

.
$\sigma(1) = 3,\ \sigma^2(1) = 3 \Rightarrow O\sigma(1) = \{1, 3\} = O\sigma(3)$
$\sigma(2) = 4,\ \sigma(4) = 5,\ \sigma(5) = 2 \Rightarrow O\sigma(2) = \{2, 4, 5\} = O\sigma(4) = O\sigma(5)$

Definizione di Ciclo: Una permutazione $\sigma \in \mathfrak{S}_n$ è un ciclo se ha un'unica orbita non banale (cioè di cardinalità > 1)

Esempio:
$\sigma(1) =$

.

$\sigma(2) =$

.

Si ha che $\sigma(1)$ e $\sigma(2)$ sono cicli.
σ dell'esempio precedente non è un ciclo, ma ne è la composizione.

Notazione: Indico un ciclo S con la notazione $(i, s(i), s^2(i), \dots, s^{k-1}(i))$, $k =$ ordine di S

Esempio:
$\sigma_1 = (1, 3)$ e $\sigma_2 = (2, 4, 5)$ dell'esempio precedente

Osservazioni:

1. Tale scrittura non è unica: $\sigma(1) = (1, 3) = (3, 1)$ e $\sigma(2) = (2, 4, 5) = (4, 5, 2) = (5, 2, 4)$
2. σ non è un ciclo, ma posso scriverlo come $\sigma = \sigma_1 \circ \sigma_2 = (1, 3) \circ (2, 4, 5)$. Però è commutativo, ossia non importa l'ordine in quanto sono cose indipendenti. $\sigma = \sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$
3. Ogni permutazione $\sigma \in \mathfrak{S}_n$ può essere scritto come composizione di cicli, uno per ciascuna sua orbita.

Esempio:
1.
Sia $\sigma \in \mathfrak{S}_8$

.

Si ha che $\sigma_1 = (1,3,7,4),\ \sigma_2 = (2,6),\ \sigma_3 = (5),\ \sigma_4 = (8)$, quindi $\sigma = (1,3,7,4)(2,6)$
2.
Sia $\mathfrak{S}_3$

$id =$ $s_1 =$ $= (1,2)$

$s_2 =$ $= (2,3)$ $t =$ $= (1,3)$

$c =$ $= (1,2,3)$ $c^{-1} =$ $= (1,3,2)$

Sono tutti ciclici ma non è un caso (perché n è un numero piccolo)

Definizione di Trasposizione: Una Trasposizione, o Scambio, è un ciclo di lunghezza 2

Esempio:
Le trasposizioni di $\mathfrak{S}_3$ sono $(1,2),(1,3),(2,3)$.
Invece $(1,2,3),(1,3,2)$ non sono trasposizioni, ma abbiamo osservato che si scrivono come composizioni di trasposizioni.
$(1,2)(1,3) = (2,3,1) = (1,2,3)$ e $(2,3)(1,2) = (1,3,2)$
Le trasposizioni si leggono da sinistra a destra, le composizioni da destra a sinsitra
Esempio:
$\sigma = (1,4,3,2,5) \in \mathfrak{S}_5 \Leftrightarrow (1,5)(1,2)(1,3)(1,4) = (1,4,3,2,5)$

Proposizione: Ogni permutazione $\sigma \in \mathfrak{S}_n$ si scrive come composizione di trasposizioni.
Dimostrazione:
Poiché ogni permutazione è composizione di cicli, basta verificare di ogni ciclo è composizione di trasposizioni. In effetti sia $\sigma = (i_1, i_2, \dots, i_k)$ per qualunque ciclo. Allora $\sigma = (i_1, i_k)(i_1, i_{k-1})\dots(i_1, i_2)$

Definizione di Trasposizione Semplice/Elementare: Una trasposizione Semplice o Elementare è una trasposizione della forma (a,b), *Con un esempio, sia* $\mathfrak{S}_n$ $s_1 = (1,2),\ s_2 = (2,3), \dots,\ s_{n-1}(n-1,n)$

Teorema: $\mathfrak{S}_n$ è generato da $s_1, s_2, \dots, s_{n-1}$
Esempio:
1. $t = (1,3) = (1,2)(2,3)(1,2) = s_1 \circ s_2 \circ s_1$
2. $\tau \in \mathfrak{S}_7,\ \ \tau = (2,6) \quad \tau = (2,3)(3,4)(4,5)(5,6)(4,5)(3,4)(2,3)$

Dimostrazione:
Poiché ogni permutazione è composizione di cicli e ogni ciclo è composizione di trasposizioni, basta dimostrare che ogni trasposizione è composizione di trasposizioni semplici.
In effetti $(i,k) = (i,i+1)(i+1,i+2)\dots(k-1,k)\dots(i+1,i+2)(i,i+1) = s_i s_{i+1}\dots s_{k-2}s_{k-1}s_{k-2}\dots s_{i+1}s_i$

Proposizione: L'ordine di un ciclo di lunghezza m è m, l'ordine di una permutazione è il mcm delle lunghezze dei cicli
Esempio:
$|(1,2,3)(4,5)| = 6$
Dimostrazione:
Sia $a > 1$ e sia $\sigma = \sigma_1\dots\sigma_k$, dove $\sigma_1,\dots,\sigma_k$ sono cicli. Poiché questi sono commutativi tra loro, $\sigma^a = \sigma_1^a\dots\sigma_k^a$ e poiché lavorano su orbite distinte $\sigma^a = id \Leftrightarrow \sigma_1^a = id,\dots,\sigma_k^a = id \Leftrightarrow a$ è divisibile per l'ordine di ciascun σ_i e dunque per il loro mcm
Esempio:
$\sigma = (1,2,3)(4,5) \Rightarrow \sigma^a = (1,2,3)^a(4,5)^a$ e $\begin{cases}(1,2,3)^a = id \Leftrightarrow 3|a\\(4,5)^a = id \Leftrightarrow 2|a\end{cases} \Rightarrow \sigma^a = id \Leftrightarrow 6|a$

Definizione di Simplesso: In $\mathbb{R}^n$ consideriamo il sottospazio affine (traslato) di equazione $x_1 + x_2 + \dots + x_n = 1$. Il *Simplesso* di dimensione $n-1$ è l'indieme $\Delta_{n-1}\{(x_1,\dots,x_n) \in V \mid x_1 \geq 0, x_2 \geq 0, \dots, x_n \geq 0\}$

Esempi:
1. Con $n = 2$ si ha che $V = x_1 + x_2 = 1$ con $x_1 \geq 0 \wedge x_2 \geq 0$. Questo rappresenta un segmento di vertici $(1,0)$ e $(0,1)$, la cui unica simmetria non banale è quella rispetto al punto medio
2. Con $n = 3$ si ha che $V = x_1 + x_2 + x_3 = 1$ con $x_1 \geq 0 \wedge x_2 \geq 0 \wedge x_3 \geq 0$. Questo rappresenta un triangolo equilatero di vertici $(1,0,0)$, $(0,1,0)$ e $(0,0,1)$. Il suo gruppo di simmetrie è $\mathfrak{D}_3 \simeq \mathfrak{S}_3$
3. Con $n = 4$ si ha che $V = x_1 + x_2 + x_3 + x_4 = 1$ con $x_1 \geq 0 \wedge x_2 \geq 0 \wedge x_3 \geq 0 \wedge x_4 \geq 0$. Questo rappresenta un tetraedro (dado a 4 facce) di vertici $(1,0,0,0)$, $(0,1,0,0)$, $(0,0,1,0)$ e $(0,0,0,1)$

Teorema: Il gruppo G dei movimenti rigidi che mandano il Simplesso Δ_{n-1} in sé stesso è il gruppo simmetrico $\mathfrak{S}_n$
Dimostrazione:
Ogni trasformazione geometrica che manda Δ_{n-1} in sé stesso permutando i suoi vertici $e_1,\dots,e_n$. Quindi possiamo vedere G come un sottogruppo di $\mathfrak{S}_n$.
Osserviamo che $\forall i \in \{1,\dots,n-1\},\ S_i = (i,i+1)$ che scambia l'i-esima coordinata con la $i+1$-esima coordinata, lasciando invariata l'equazione $x_1 + x_2 + \dots + x_n = 1$, Quindi $s_i \in G,\ \forall i \in \{1,\dots,n\}$.
Cioè $G \leq \mathfrak{S}_n$, G contiene $s_1,\dots,s_{n-1}$. Ma tali elementi generano G. Quindi $G = \mathfrak{S}_n$

Abbiamo visto che $\forall\sigma \in \mathfrak{S}_n$ è composizione di trasposizioni

Definizione di σ Pari/Dispari: σ è pari se può essere scritto come composizione di un numero pari di trasposizioni, σ è dispari se può essere scritto come composizione di un numero dispari di trasposizioni.

Esempi:
$id = (1,2)(1,2)$ è pari
Tutte le trasposizioni sono dispari
$(1,2,3) = (1,3)(1,2)$ è pari
$(1,3,2,4) = (1,4)(1,2)(1,3)$ è dispari
$(1,3,2,4)(5,7,6) = (1,4)(1,2)(1,3)(5,6)(5,7)$ è dispari

Dato un polinomio p in n variabili $p(x_1,\dots,x_n)$ e dato $\sigma \in \mathfrak{S}_n$, definiamo σp il polinomio $\sigma p(x_1,\dots,x_n) = p(x\sigma_1,\dots,x\sigma_n)$ cioè σ agisce su tutte le variabili.

Esempio:
1. $p_1(x_1,x_2,x_3) = x_1 + x_2^2 - 3x_3$ $(1,2,3)p(x_1,x_2,x_3) = x_2 + x_3^2 - 3x_1$
2. $p(x_1,\dots,x_5) = \underset{\Longleftrightarrow}{\underbrace{(x_1-x_2)}_{1}}\underbrace{(x_1-x_3)}_{\times}\underset{\Longleftrightarrow}{\underbrace{(x_1-x_4)}_{1}}\underbrace{(x_1-x_5)}_{\times}\underbrace{(x_2-x_3)}_{\cdot}\underbrace{(x_2-x_4)}_{*}\underset{\Longleftrightarrow}{\underbrace{(x_2-x_5)}_{2}}\underbrace{(x_3-x_4)}_{\cdot}\underbrace{(x_3-x_5)}_{\times}\underset{\Longleftrightarrow}{\underbrace{(x_4-x_5)}_{2}}$
Con $(2,4)p(x_1,\dots,x_5)$ si ottiene che quelli con $\times$ restano invariati, quelli con $\Leftrightarrow$ si scambiamo (quelli con lo stesso numero), quelli con $\cdot$ cambiano di segno ma si annullano, quello con $*$ invece cambia segno e fa cambiare segno al polinomio.

Definizione: $p(x_1,\dots,x_n) = \prod_{1 \leq i < j \leq n}(x_i - x_j)$

Lemma: Sia $\tau \in \mathfrak{S}$ una trasposizione. Allora $\tau p(x_1, \dots, x_n) = -p(x_1, \dots, x_n)$
Dimostrazione:
Il prodotto contiene fattori invariati (che non contengono né i né j) e restano invariati ($\times$), fattori che vengono scambiati tra loro ($\Leftrightarrow$) $(x_h - x_i)(x_h - x_j) \forall h < i, (x_i - x_h)(x_j - x_h), \forall h > j$, fattori che sono scambiati fra loro con cambio di segno che si semplifica ($\cdot$) $i < h < j (x_i - x_h)(x_h - x_j) \overset{\tau}{\mapsto} (x_j - x_h)(x_h - x_i)$, poi c'è $(x_i - x_j)$ che cambia di segno.

Teorema: Una permutazione può essere pari se è dispari.
Dimostrazione:
Supponiamo per assurdo che lo sia, cioè che $\sigma \in \tau_1 \circ \dots \circ \tau_n = t_1 \circ \dots \circ t_n$ e sia
$\sigma p(x_1, \dots, x_n) = (-1)^{2a} p(x_1, \dots, x_n) = (-1)^{2a+1} p(x_1, \dots, x_n) \Rightarrow p(x_1, \dots, x_n) = -p(x_1, \dots, x_n)$ e ciò è assurdo perché $p(x_1, \dots, x_n) \neq 0$

Definizione di Segno di σ: Il segno di σ è $\varepsilon(\sigma) = (-1)^{\text{Pari o dispari } \sigma} = \begin{cases} 1 \text{ se } \sigma \text{ è pari} \\ -1 \text{ se } \sigma \text{ è dispari} \end{cases}$

Osservazione: $\varepsilon : \begin{matrix} \mathfrak{S}_n & \to & \{+1, -1\} \\ \sigma & \mapsto & \varepsilon(\sigma) \end{matrix}$ è un omomorfismo tra $(\mathfrak{S}_n, \circ)$ e $(\{+1, -1\}, \circ)$. $Ker(\varepsilon) = \{\text{Permutazioni pari}\}$ è sottogruppo di $\mathfrak{S}_n$ che si indica con $\mathscr{A}_n$ e si chiama *Alterno*

Esempio:
$\mathfrak{S}_3 = \{(1,2), (2,3), (1,3), \underbrace{(1,2,3)(1,3,2), id}_{\in \mathscr{A}_3}\}$

Proposizione: $|\mathscr{A}_n| = \frac{n!}{2}$, cioè le permutazioni pari sono tante quante quelle dispari.
Dimostrazione:
$m_{(1,2)} : \begin{matrix} \mathfrak{S}_n & \to & \mathfrak{S}_n \\ \sigma & \mapsto & (1,2)\sigma \end{matrix}$ è biunivoca (teorema di Cayley) e σ è pari $\Leftrightarrow (1,2)\sigma$ è dispari. Quindi $m_{(1,2)}$ mette in biezione $\{\text{Permutazioni Pari}\} \to \{\text{Permutazioni Dispari}\}$

D'ora in avanti indicheremo l'operazione di un gruppo astratto con $\cdot$ invece di $\star$. Di conseguenza $g_1 \star g_2 \to g_1 g_2$ e l'inverso di un elemento g con g^{-1} al posto di $\tilde{g}$.
Possiamo quindi riformulare tutto questo nuovo linguaggio, ad esempio $f : G \to H$ è un omomorfismo se $f(g_1 g_2) = f(g_1) f(g_2) \ \forall g \in G$

Definizione di Coniugio: Sia G un gruppo e $h \in G$. Il Coniugio per h è l'applicazione $C_h : \begin{matrix} G & \to & G \\ g & \mapsto & hgh^{-1} \end{matrix}$. Nella vecchia notazione sarebbe $h \star g \star g^{-1}$

Proposizione: Proprietà del Coniugio:

1. $(C_{h_2} \circ C_{h_1}) = C_{h_2 h_1}$
2. C_h è un automorfismo di $G, \forall h \in G$
   Dimostrazione:
   1. $(C_{h_2} \circ C_{h_1})(g) = (C_{h_2}(C_{h_1}(g))) = C_{h_2}(h_1 g h_1^{-1}) = \underbrace{h_2 h_1}_{\in G} g \underbrace{h_1^{-1} h_2^{-1}}_{(h_2 y_1)^{-1}} = C_{h_1 h_2}(g), \forall g \in G$
   2. Dobbiamo dimostrare che C_h, è biunivoca ed è un omomorfismo.
   C_h è biunivoca perché la sua funzione inversa è $C_{h^{-1}}$ (il -1 è all'h)
   Infatti $(C_{h^{-1}} \circ C_h)(g) = (C_{h^{-1}h})(g) = C_{id}(g) = ege = g, \forall g \in G$
   Infatti $(C_{h^{-1}} \circ C_h) = (C_{h^{-1}h}) = C_{id} = e$
   In alternativa avremmo potuto osservare che C_h è iniettiva perché se $C_h(g_1) = C_h(g_2) \Rightarrow$
   $\Rightarrow hg_1h^{-1} = hg_2h^{-1} \xRightarrow{\text{Legge della Cancellazione}} g_1h^{-1} = g_2h^{-1} \Rightarrow g_1 = g_2$, ossia è iniettiva.
   Quindi $C_h : G \to G$ è anche suriettiva per ragioni di cardinalità (stesso numero di elementi). Inoltre $C_h(g_1) C_h(g_2) = (hg_1h^{-1})(hg_2h^{-1}) = hg_1g_2h^{-1} = C_h(g_1g_2)$ Quindi è omomorfismo

Definizione di Essere Coniugati: $g_1, g_2 \in G$ sono coniugati se $\exists h \in G$ t.c. $C_h(g_1) = g_2$

Osservazione: È una relazione di equivalenza (sul foglio di esercizi). Le classi di equivalenza sono dette classi di coniugio.

Esempi:
1. Se G è commutativo (o abeliano) allora $hgh^{-1} = hh^{-1}g = g$, ovvero $C_h = id, \forall g \in G$. Infatti ogni elemento di G è coniugato a se stesso.

2. Se $G = GL(n, \mathbb{K}) = \{\text{Matrici n} \times \text{n invertibili}\}$, il coniugio è detto similitudine.
$M_2 = C_B(M_1) = BM_1B^{-1} \Leftrightarrow M_1, M_2$ rappresentano la stessa applicazione lineare in basi diverse e B è detta la matrice del cambiamento di base.
3. Se $G = \mathfrak{D}_n$ diedrale $=\{r^k\} \cup \{r^k s\}$ con $k \in \{0, \dots, n-1\}$.
Se $x = r^k \to C_r(x) = rr^kr^{-1} = r^k = x$
Se $x = r^k \to C_s(x) = \underbrace{sr^k}s^{-1} = r^{-k}ss = r^{-k} = x^{-1}$
Se $x = r^k s \to C_r(x) = rr^k\underbrace{sr^{-1}} = rr^krs = r^{k+2}s$
Se $x = r^k s \to C_s(x) = sr^kss^{-1} = sr^k = r^{-1}s$
4. $G = \mathfrak{S}_n$ è l'esempio che vedremo più nel dettaglio

Esempio dell'esempio:
Sia $\sigma = (1374)$ e $\tau = (12)(35)(764)$
Si ha $C_\tau(\sigma) = \tau\sigma\tau^{-1} = (12)(35)(764)(1374)(12)(35)(746) = (1)(2567)(3)(4) = (2567)$
Basta vedere che $1 \to 2, 3 \to 5, 7 \to 6, 4 \to 7$ che è esattamente τ

Lemma Estremamente Importante per dopo: Sia $\sigma = (i_1, \dots, i_k)$ un k-ciclo e sia $\tau \in \mathfrak{S}_n$ una permutazione qualsiasi. Allora anche $C_\tau(\sigma)$ sarà un k-ciclo, precisamente è il k-ciclo dato da $C_\tau = (\tau(i_1), \dots, \tau(i_k))$
Dimostrazione:
Per ogni $j \in \{1, \dots, n\}$ vogliamo calcolare $C_\tau(\sigma)(j) = \tau\sigma\tau^{-1}(j)$. Distinguiamo 2 casi:
1. Se j non è in $\tau(i_h)$ per nessun h allora $\tau^{-1}(j)$ non è in nessun h, allora σ lo lascia invariato e quindi $\tau\sigma\tau^{-1}(j) = \tau\tau^{-1}(j) = j$
2. Se invece esiste h tale che $j = \tau(i_h)$, allora $\tau\sigma\tau^{-1}(j) = \tau\sigma(i_h) = \tau(i_{h+1})$ dove $h = n$, allora $i_{n+1} = i_1$
Quindi $\tau\sigma\tau^{-1}$ è il k-ciclo che avevamo detto e vale $(\tau(i_1), \dots, \tau(i_n))$

Definizione di Partizione di un Numero: Sia $n \in \mathbb{N}, n > 0$. Una partizione di n è la successione di λ, $(\lambda_1, \lambda_2, \lambda_3, \dots)$ con $\forall i \in \mathbb{N}, \lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \dots$ con $\sum \lambda_i = n$

Esempi:
Le partizioni di 3 sono:
- $(3, 0, 0, 0, 0, 0, 0, \dots) = (3)$
- $(2, 1, 0, 0, 0, 0, 0, \dots) = (2, 1)$
- $(1, 1, 1, 0, 0, 0, 0, \dots) = (1, 1, 1)$

Osservazione: Diciamo che $\sigma \in \mathfrak{S}_n$ ha strutture cicliche λ se le sue orbite, ordinate di cardinalità decrescente hanno cardinalità $\lambda_1, \lambda_2, \lambda_3, \dots$

Esempio:
- $(3) = (1, 2, 3)$ e $(1, 3, 2)$ 3-cicli
- $(2, 1) = (1, 2), (1, 3), (2, 3)$ Trasposizioni
- $(1, 1, 1) =$ Identità

Teorema: Due elementi di $\mathfrak{S}_n$ sono coniugati $\Leftrightarrow$ hanno stessa struttura ciclica. Quindi le classi di coniugo di $\mathfrak{S}_n$ sono in biezione con le partizioni di n.
Dimostrazione:
Siano σ_1 e σ_2 due permutazioni con struttura ciclica $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_r)$ dove λ_r rappresenta l'ultimo λ non nullo.
Quindi $\sigma_1 = (a_{1,1}, \dots, a_{1,\lambda_1})(a_{2,1}, \dots, a_{2,\lambda_2})\dots(a_{r,1}, \dots, a_{r,\lambda_r})$ e $\sigma_2 = (b_{1,1}, \dots, b_{1,\lambda_1})(b_{2,1}, \dots, b_{2,\lambda_2})\dots(b_{r,1}, \dots, b_{r,\lambda_r})$.
Considero $\tau \in \mathfrak{S}_n$ tale che $\tau(a_{1,1}) = b_{1,1}$ e così via $tau(a_{r,\lambda_r}) = b_{r,\lambda_r}$. Poiché σ_1 è un prodotto di cicli e poiché C_τ è un omomorfismo, basta calcolare C_τ per ciascun ciclo, che per il lemma precedente $C_\tau(\sigma_1) = \sigma_2$
Quindi se σ_1 e σ_2 hanno la stessa struttura ciclica sono coniugate.
D'altra parte sempre per il lemma, data una permutazione σ_1 e $\tau \in \mathfrak{S}_n$, $C_\tau(\sigma_1)$ ha la stessa struttura ciclica di σ_1

Esempio:
Sia $n = 4$

$$\left.\begin{array}{c|c|c|c|c} \text{Partizione} & \text{Elementi} & \text{Ordine} & \text{Parità} & \text{Numero} \\ (4) & (1234) & 4 & D & 6 \\ (3,1) & (123) & 3 & P & 8 \\ (2,2) & (12)(34) & 2 & P & 3 \\ (2,1,1) & (12) & 2 & D & 6 \\ (1,1,1,1) & Id & 1 & P & 1 \end{array}\right\}\text{In tutto sono } 4! = 24$$

Esempio:
Siano $\sigma_1 = (137)(24)(56)$ e $\sigma_2 = (457)(26)(13) \in \mathfrak{S}_7$
Trovare τ tale che $C_\tau(\sigma_1) = \sigma_2$
τ esiste perché σ_1 e σ_2 hanno la stessa struttura e vale $(3,2,2)$
Infatti τ vale (14635)
basta mettere i due cicli uno sotto l'altro e torna

Osservazione: τ non è unico, dipende da come sono scritti i cicli.

Definizione di Laterale Sinistro: Sia G un gruppo, sia $H \leq G$ un sottogruppo e sia $g \in G$. L'insieme $gH = \{gh,\ h \in H\}$ è detto classe laterale sinistro (o semplicemente laterale sinistro) di g.

Esempi:
1. $(\mathbb{Z},+) = G$ e $H = n\mathbb{Z} = \{\text{Multipli di } n \text{ con } n \in \mathbb{N}\}$. Per esempio con $n=1$ si ha che $1H = \{1+h, h \in n\mathbb{Z}\} = \{m \in \mathbb{Z} \mid m \equiv 1\ (n)\} = [1] \in \mathbb{Z}_{/N}$. Analogamente si può fare la stessa cosa con qualsiasi elemento n.
2. $G = U_8 = \{[1],[3],[-3],[-1]\}$ e $H = \{[1],[-1]\}$. H è un sottogruppo rispetto alla moltiplicazione. Si ottiene che $[1]H = H = [-1]H$. Si ottiene inoltre che $[3]H = \{[3][1],[3][-1]\} = \{[3],[-3]\} = [-3]H$
3. $G = \mathfrak{D}_n$ e $H = R_n = \{r^k, \forall k \in \mathbb{Z}\}$. $r^kH = H$ ossia tutte le rotazioni. $sH = \{sr^k, \forall k \in \mathbb{Z}\} = \{\text{Tutte le simmetrie}\}$. Ma la cosa sarebbe stata uguale con tutte le simmetrie.

Lemma:

1. I laterali sinistri formano una partizione di G
2. Ciascun laterale ha la stessa cardinalità do H
   Dimostrazione:
   1. Poiché $g \in gH$, i laterali sono non vuoti e la loro unione è G. Dobbiamo dimostrare che sono a 2 a 2 disgiunti, cioè $\forall g_1, g_2 \in G$ o $g_1H = g_2H$ o $g_1H \cap g_2H = \varnothing$. Supponiamo che $g_1H \cap g_2H \neq \varnothing$, questo implica che $\exists x \in g_1H \cap g_2H \Rightarrow \Rightarrow \exists h_1, h_2 \in H\ t.c.\ x = g_1h_1 = g_2h_2 \Rightarrow g_1 = g_2h_2h_1^{-1}$. Sia $k \in g_1H \Rightarrow \exists h \in H\ t.c.\ k = g_1h$, ma per quanto abbiamo definito poco fa si ha che $k = g_1h = (g_2h_2h_1^{-1})h = g_2\underbrace{h_2h_1^{-1}h}_{\in H} \Rightarrow k \in g_2H$
   2. Considero l'applicazione $\begin{array}{ccc} H & \to & gH \\ h & \mapsto & gh \end{array}$, è suriettiva per definizione di laterale. È iniettiva? Si per la legge di cancellazione $gh_1 = gh_2 \Rightarrow h_1 = h_2$. Quindi è biunivoca, quindi hanno la stessa cardinalità

Definizione di Indice: Il numero di classi laterali sinistre gH è detto indice di H in G e si indica con $[G:H]$

Teorema di Lagrange: Sia G in un gruppo finito. $|G| = |H| \cdot [G:H] \Rightarrow |H| \text{ Divide } |G|$ ^6c4790
Dimostrazione:
Per il lemma precedente ci sono $[G:H]$ laterali, tra loro disgiunti con cardinalità $|H|$ e la loro unione è G.

Conseguenze del Teorema di Lagrange:

1. Corollario 1: L'ordine di ogni elemento di G divide $|G|$
   Dimostrazione:
   $\forall g \in G, \langle g \rangle$ è sottogruppo ciclico di G. $|\langle g \rangle| = o(g)$ deve dividere G
2. Corollario 2: Se $|G|$ è primo, allora G è ciclico
   Dimostrazione:
   Sia $g \neq id$. Dunque $o(g) \neq 1$ e per il corollario 1 $o(g)|p \Rightarrow o(g) = p \Rightarrow \langle g \rangle$ ha p elementi ed è uguale a G
3. Il teorema di Eulero stesso.
   Dimostrazione:
   Basta applicare il Corollario 1 a $G = U_n$ infatti $|G| = \phi(n)$. Ci dice che $\forall [n] \in U_n,\ [a]^{\phi(n)} = [1]$. Ovvero che $\forall a \in \mathbb{Z}$ t.c. $\mathcal{MCD}(a,n) = 1 \Rightarrow a^{\phi(n)} = 1\ (n)$

Definizione di Laterale Destro: Siano $H \leq G$ e $g \in G$. Definisco Laterale Destro $Hg = \{hg \mid h \in H\}$

Osservazione: I laterali destri formano un partizione di G e ciascuno di esso ha cardinalità $h = |H|$
Si dimostra come per il Laterale Sinistro. Di conseguenza il numero di Laterali Destri è uguale al numero di Laterali Sinistri $[G:H]$

Esempio:
$G = \mathfrak{S}_3$ e $H = \{id, (12)\}$

Quindi ci sono $\frac{|G|}{|H|} = 3$ laterali sinistri:
$idH = H = (12)H$
$(23)H = \{(23)id, (23)(12)\}) = \{(23), (132)\} = (132)H$
$(13)H = \{(13)id, (13)(12)\} = \{(13), (123)\} = (123)H$
e ci sono 3 laterali destri:
$Hid = H = H(12)$
$H(23) = \{id(23), (12)(23)\} = \{(23), (123)\} = H(123)$
$H(13) = \{id(13), (12)(13)\} = \{(13), (132)\} = H(132)$

Definizione di Sottogruppo Normale: Diciamo che $H \leq G$ è normale se i laterali destro e sinistro coincidono e si indica con $H \trianglelefteq G$

Esempi:
1. $\{id, (12)\}$ $\underline{non}$ è normale in $\mathfrak{S}_3$
2. Se G è commutativo, tutti i sottogruppi sono normali.
3. I sottogruppi banali $\{e\}$ e $\{g\}$ sono sottogruppi normali.
4. Sia G un gruppo e H un sottogruppo di indice 2, ossia che $[G : H] = 2$. Questo implica che ci sono 2 laterali sinistri $H, G \setminus H$ e per la stessa ragione ci sono due laterali destri: $H, G \setminus H$. Quindi $H \trianglelefteq G$
5. In particolare $R_n \trianglelefteq \mathfrak{D}_n$
6. $\mathscr{A}_n \trianglelefteq \mathfrak{S}_n$ perché ha indice 2
7. $G = \mathfrak{D}_4 = \{r, r^2, r^3, r^4 = id, s, rs, r^2s, r^3s\}$ e $H = \{id, r^2\}$. Ci sono $\frac{|G|}{|H|} = 4$ laterali.
$idH = \{id, r^2\} = Hid$
$rH = \{r, r^3\} = Hr$
$sH = \{sid, sr^2\} = \{s, r^{-2}s\} = \{s, r^2s\} = Hs$
$rsH = \{rsid, rsr^2\} = \{rs, r^3s\} = Hrs$
Quindi $H \trianglelefteq G$

Definizione di Centro di G: Dato un gruppo G, si definisce il centro di G con $Z(G) = \{z \in G \mid zg = gz, \forall g \in G\}$

Esempio:
$Z(\mathfrak{D}_4) = \{id, r^2\}$

Osservazione: $Z(G)$ è sottogruppo normale in G
Dimostrazione:
$\forall g \in G,\ gZ(G) = \{gz, z \in Z(G)\} = \{zg, z \in Z(G)\} = g$

Proposizione: Un sottogruppo è normale se e solo se è unione di due classi di coniugio.
Dimostrazione:
Sia $N \leq G$, N è normale $\Leftrightarrow \forall g \in G, gN = Ng \Leftrightarrow gNg^{-1} = N \forall g \in G$. Ma $gNg^{-1} = \{gng^{-1}, n \in N\} \Leftrightarrow gng^{-1} \in N, \forall g \in G$ cioè $\forall n \in N, N$ contiene tutti i coniugati di N, infatti $gng^{-1} = C_g(n)$. Quindi N è unione di classi di coniugio.

Esempio:
1. In $\mathfrak{S}_4$ il sottogruppo N è $\{\underbrace{id}_{1,1,1,1}, \underbrace{(12)(34), (13)(24), (14)(23)}_{2,2}\}$. N è quindi unione di classi di coniugio, quindi $N \trianglelefteq G$
2. In $\mathfrak{S}_3$, $H = \{id, (12)\}$ non è normale perché contiene (12) ma non i suoi coniugati (13) e (23)
3. $\mathscr{A}_n \trianglelefteq \mathfrak{S}_n$ perché se $\sigma \in \mathscr{A}_n$ tutti gli elementi con la stessa struttura di σ sono pari.

Quindi, dato un omomorfismo $f : G \to H$, abbiamo definito $Ker(f)$ come $\{g \in G \mid f(g) = 0\}$

Proposizione: $Ker(f) \trianglelefteq G$
Dimostrazione:
Abbiamo già verificato che era sottogruppo $Ker(f) \leq G$
Sia $n \in Ker(f)$, dobbiamo mostrare che $gng^{-1} \in Ker(f), \forall g \in G$ (e ciò la rende vera per la proposizione precedente).
In effetti poiché $f(n) = e_H \Rightarrow f(gng^{-1}) = f(g)\underbrace{f(n)}_{=0}f(g^{-1}) = f(g)f(g^{-1}) = e_H$

Osservazione: Sia $H \leq G$, allora x, y sono nello stesso laterale destro se e solo se $xy^{-1} \in H$.
Infatti se $xy \in Hg \Rightarrow x = h_1g; y = h_2g \Rightarrow y^{-1} = (h_2g)^{-1} = g^{-1}h_2^{-1}$
$\Rightarrow)$ $xy^{-1} = h_1gg^{-1}h_2^{-1} = h_1h_2^{-1} \in H$. $\Leftarrow)$ Viceversa se$xy^{-1} \in H \Rightarrow xy^{-1} = h \Rightarrow x = hy \Rightarrow x \in Hy$

Vogliamo ora mostrare che se N è normale, l'insieme dei suoi laterali è un gruppo.

Definizione di Compatibilità: Sia G un gruppo e $\sim$ una relazione di equivalenza su G. Diciamo che $\sim$ è compatibile con l'operazione di G se $\forall x, x', y, y' \in G$, $x \sim x', y \sim y' \Rightarrow xy \sim x'y'$

Esempio:
In $(\mathbb{Z}, +)$, la relazione di equivalenza $x \sim y \Leftrightarrow x \equiv y\ (n)$ è compatibile perché se $x \equiv x', y \equiv y' \Leftrightarrow x + y \equiv x' + y'\ (n)$
Questo ci ha permesso di definire la somma fra classi

Sia G un gruppo e $\sim$ una relazione di equivalenza compatibile. Possiamo definire sull'insieme quoziente $G_{/\sim}$ un'operazione $[x]\underbrace{}_{\text{Operazione compatibile}}[y] = [x\underbrace{}_{\text{Operazione di } G}y]$

Proposizione: Questa operazione è ben definita e rende $G_{/\sim}$ un gruppo.
Dimostrazione:
Ben definita perché se $[x] = [x']$ e $[y] = [y']$, allora perché poiché questa è compatibile, $[xy] = [x'y']$
È un gruppo perché $[e]$ è l'elemento neutro, $[g]^{-1} = [g^{-1}], \forall g \in G$ e la nuova operazione eredità l'associatività dell'operazione in G

Teorema:

1. Se $N \trianglelefteq G$, allora la relazione "$x \sim y \Leftrightarrow x$ e y appartengono alla stessa classe laterale" è una relazione di equivalenza.
2. Se una relazione di equivalenza è compatibile, allora $[e]$ è un sottogruppo normale di G e $x \sim y \Leftrightarrow x$ e y appartengono allo stesso laterale
   Dimostrazione:
   1. Dato un sottogruppo N (normale o no) se laterali formano una partizione di G, quindi appartenere allo stesso laterale è una relazione di equivalenza. Se $N \trianglelefteq G$ mostriamo che è compatibile. Siano $\underbrace{x' \sim x^{-1}}_{x'x^{-1} \in N}, \underbrace{y' \sim y^{-1}}_{y'y^{-1} \in N} \in G \Rightarrow \exists n \in N\ t.c.\ x'x^{-1} = n \Rightarrow x' = nx$. Voglio mostrare che
   Voglio mostrare che $xy \sim x'y'$, ovvero che $xy \sim (xy)^{-1} \in N$. In effetti $x'y'y^{-1}x^{-1} = n\, \overbrace{x\, \underbrace{y'y^{-1}}_{\in N}\, x^{-1}}^{\in N} \in N$. Poiché N è normale tutto sta in N.
   2. Sia G un gruppo e $\sim$ una relazione di equivalenza compatibile. $N = [e]$ è un sottogruppo di G poiché $e \in [e]$. Se $n \in [e] \Rightarrow n \in e \Rightarrow n^{-1}n \sim n^{-1}e \Rightarrow e \sim n^{-1} \Rightarrow n^{-1} \in [e]$. $n_1, n_2 \in [e] \Rightarrow n_1 \sim e, n_2 \sim e \Rightarrow n_1n_2 \sim ee = e \Rightarrow n_1, n_2 \in N$.
   Normalità: sia $n \in N$ e $g \in G$, allora $gng^{-1} \sim geg^{-1} = e \Rightarrow C_g(n) \in N \Rightarrow N$ è normale.
   Inoltre $x \sim y \Leftrightarrow xy^{-1} \sim yy^{-1} = e \Leftrightarrow xy^{-1} \in [e]$, dunque sono nello stesso laterale e viceversa (se x, y sono nello stesso laterale, allora $xy^{-1} \in [e] \Rightarrow xy^{-1} \sim e \Rightarrow xy^{-1} \sim yy^{-1} \Rightarrow x \sim y$)

Osservazione: Se N è normale, ho una relazione di equivalenza compatibile, le cui classi di equivalenza sono proprio i laterali.

Definizione di Gruppo Quozionete: Quindi $G_{/N} = \{\text{Laterali di } N\}$ è un gruppo, detto Quoziente con operazione data da $g_1N \cdot g_2N = g_1g_2N$

Esempio:
1. Abbiamo visto che $N = \{id, r^2\}$ è normale in $\mathfrak{D}_4$, ci sono 4 classi laterali e quindi $G_{/N} = \{N, rN, sN, rsN\}$, ovvero $G_{/\simeq} = \{[id], [r], [s], [rs]\}$ è un gruppo i cui elementi hanno ordine due, quindi è isomorfo al gruppo di Klein K_4
2. $\mathfrak{S}_{4/K_4}$
3. $\mathbb{Z}_{/n\mathbb{Z}} = \mathbb{Z}_{/n}$
4. Quoziente di uno spazio vettoriale V per un sottospazio U
5. $G = \mathfrak{S}_n$ e $H = \mathscr{A}_n$, siano $\sigma_1 \sim \sigma_2 \Leftrightarrow \sigma_1$ e σ_2 hanno lo stesso segno (Pari/Dispari). Quindi $G_{/N} = \mathfrak{S}_{n/\mathscr{A}_n} = \{id, (12)\} \simeq (\{1, -1\}, \cdot) \simeq \mathbb{Z}_{/2}$
6. $G = \mathfrak{D}_n$ e $N = R_n$: $\mathfrak{D}_{n/R_n} = \{R_n, sR_n\} = \{[id], [s]\} \simeq R_2 \simeq \mathbb{Z}_2$

Teorema Fondamentale di omomorfismi tra gruppi: Sia $f : G \to H$ un omomorfismo di gruppi. Allora l'applicazione
$$\begin{array}{rcl} G_{/Ker(f)} & \to & Im(f) \\ \overline{f} : gKer(f) & \mapsto & f(g) \\ [g] & \mapsto & f(g) \end{array}$$ è isomorfismo.
Dimostrazione:
Sia $N = Ker(f)$ e $\sim$ la relazione di equivalenza compatibile ad essa associata, cioè $g_1 \sim g_2 \Leftrightarrow$ sono nello stesso laterale $\Leftrightarrow [g_1] = [g_2] \Leftrightarrow f(g_1) = f(g_2)$
Quindi $\overline{f}$ è ben posta perché se $[g_1] = [g_2] \Rightarrow f(g_1) = f(g_2)$ e quindi $\overline{f}([g_1]) = \overline{f}([g_2])$

$\overline{f}$ è suriettiva perché $\forall f(g) \in Im(f)$ ho che $f(g) = \overline{f}([g])$
$\overline{f}$ è iniettiva perché se $\overline{f}([g_1]) = \overline{f}([g_2])$, allora $f(g_1) = f(g_2)$, quindi $g_1 \sim g_2 \Rightarrow [g_1] = [g_2]$
$\overline{f}$ è un omomorfimo perché f lo è: $\overline{f}([g_1][g_2]) = \overline{f}([g_1 g_2]) = f(g_1 g_2) = f(g_1)f(g_2) = \overline{f}([g_1])\overline{f}([g_2])$

Esempi:
1. Sia $G = (\mathbb{Z}, +)$ e $H = (\mathbb{C}^*, \cdot)$ e $f : \begin{matrix} G & \to & H \\ n & \mapsto & i^n \end{matrix}$
f è omomorfismo perché $i^{n+m} = i^n \cdot i^m$
Inoltre $Ker(f) \trianglelefteq G = 4\mathbb{Z} = \{\text{Multpli di 4}\}$ e $Im(f) = \{i, -1, -i, 1\} \leq H$
Per il teorema fondamentale degli omomorfismi tra gruppi $\mathbb{Z}_{/4\mathbb{Z}} = \mathbb{Z}_{/4} \xrightarrow{\sim} (\{i, -1, -i, 1\}, \cdot) \Leftrightarrow \begin{matrix} \mathbb{Z}_{/4} & \simeq & C_4 \\ [n] & \mapsto & i^n \end{matrix}$
2. SIano i gruppi $(\mathbb{R}, +)$ e $(\mathbb{R}^+, \cdot)$ con l'omomorfismo $f : \begin{matrix} \mathbb{R} & \to & \mathbb{R}^+ \\ x & \mapsto & e^x \end{matrix}$
$Ker(f) = \{0\}$ e $Im(f) =]0, +\infty[$ e per il teorema fondamentale degli omomorfismi $(\mathbb{R}, \cdot) \simeq]o, +\infty[$
3. $\varepsilon : \mathfrak{S}_n \to \mathbb{R}^+$ (segno). $Ker(f) = \mathscr{A}_n$, $Im(f) = \{+1, -1\}$ e per il TFO $\mathfrak{S}_{n/\mathscr{A}_n} \simeq \{+1, -1\}$
4. $det : GL(n, \mathbb{K}) \to \mathbb{K}^*$ è omomorfismo per il teorema di Binet. $Im(f) = \mathbb{K}^*, Ker(f) = SL(n, \mathbb{K})$. Quindi $SL(n, \mathbb{K}) \trianglelefteq GL(n, \mathbb{K})$ e ${}^{GL(n,\mathbb{K})}/_{SL(n,\mathbb{K})} \simeq \mathbb{K}^*$
5. $f : \mathfrak{D}_6 \to Sym(\{\text{Simmetrie rispetto ai vertici}\}) \simeq \mathfrak{S}_3$. f è suriettiva e $Ker(f) = \{id, r^3\}$ Per TFO $\mathfrak{D}_{6/\{id, r^3\}} \simeq \mathfrak{S}_3$

Sia G un gruppo e $N \trianglelefteq G$ e $K \trianglelefteq G$

Definizione di Prodotto Diretto: Diciamo che G è prodotto diretto di N e K se $N \cap K = \{e\}$ e $G = NK = \{nk, n \in N, k \in K\}$

Osservazione: Ogni $g \in G$ si scrive in modo unico come $g = nk$, infatti se $\exists n_1, n_2 \in N$ e $\exists k_1, k_2 \in K = g \in n_1 k_1 = n_2 k_2 \Rightarrow \Rightarrow \underbrace{n_2^{-1} n_1}_{\in N} \underbrace{k_1 k_2^{-1}}_{\in K} = ee^{-1} \in N \cap K$, ma $N \cap K = \{e\} \Rightarrow n_1 = n_2, k_1 = k_2$

Proposizione:

1. $nk = kn, \forall n \in N$ e $\forall k \in K$
2. $\varphi : \begin{matrix} G & \to & N \times K \\ nk & \mapsto & (n, k) \end{matrix}$ è isomorfismo

   Dimostrazione:
   1. Equivale a dimostrare che $knk^{-1}n^{-1} = e$. In effetti $\underbrace{nkn^{-1}}_{\in K} k^{-1} \in K \Rightarrow K \trianglelefteq G$ e $n\underbrace{kn^{-1}k^{-1}}_{\in N} \in N \Rightarrow N \trianglelefteq G$, ma $N \cap K = \{e\}$quindi $nkn^{-1}k^{-1} \in N \cap K = \{e\}$
   2. φ è ben definita e iniettiva per l'osservazione della scrittura ed è suriettiva per definizione di $N \times K$. È un omomorfismo per 1., perché $\varphi(\overbrace{g_1}^{n_1 k_1} \underbrace{g_2}_{n_2 k_2}) = \varphi(n_1 k_1 n_2 k_2) = \varphi(n_1 n_2 k_1 k_2) = (n_1 n_2, k_1 k_2)$.

Esempi:
1. $\mathbb{Z}_{/6} \simeq N \times K$ tale che $N = \{[0], [2], [4]\}$ e $K = \{[0], [3]\}$
2. $K_4 = \{id, g, h, gh\}$ è $N \times K$ tali che $N = \langle g \rangle$ e $K = \langle k \rangle$, inoltre è isomorfo a $\mathbb{Z}_{/2} \times \mathbb{Z}_{/2}$

Controesempio:
$\mathfrak{D}_n$ non è prodotto diretto di R_n e $\langle s \rangle$

Definizione di Prodotto Semidiretto: Sia G un gruppo, $H \leq G$ e $N \trianglelefteq G$, si dice che G è prodotto semidiretto di H, N e si scrive $G = N \rtimes H$ se $G = NH = \{nh, n \in N, h \in H\}$ e $N \cap H = \{e\}$

Osservazione: È ancora vero che ogni $g \in G$ si scrive in modo unico come $g = nh$, ma non è vero che $nh = hn$

Esempio:
1. $\mathfrak{D}_n = R_n \rtimes \langle s \rangle$. Infatti $R_n \rtimes \langle s \rangle$. Infatti $R_n \trianglelefteq \mathfrak{D}_n$ e $\langle s \rangle \leq \mathfrak{D}_n$
2. $\mathfrak{S}_n = \langle (12) \rangle \ltimes \mathscr{A}_n$
3. $GL(n, \mathbb{K}) = SL(n, \mathbb{K}) \rtimes \mathbb{K}^*$

Osservazione: Se $G = N \rtimes K$, allora ${}^{G}/_{N} \simeq H$

Consideriamo n carte da gioco numerate in rosso su un lato e in verde sull'altro. Diciamo che G è una trasformazione delle carte se le permuta tra loro o eventualmente ne volta qualcuna
Sia $\mathcal{B}_n = \{\text{Trasformazioni di } n \text{ carte}\}$

Osservazione: $|\mathcal{B}_n| = n! \cdot 2^n$ dove $n!$ dipende da permutazioni e 2^n voltazioni di carte.
$\mathcal{P}_n = \{g \in \mathcal{B}_n \mid g \text{ non volta nessuna carta}\} = \langle s_1, \dots, s_{n-1}\rangle$
$\mathcal{V}_n = \{g \in \mathcal{B}_n \mid g \text{ non permuta le carte (le volta e basta)}\} = \langle v_1, \dots, v_n\rangle$
Quindi $\mathcal{P}_n \leq \mathcal{B}_n$ e $\mathcal{V}_n \leq \mathcal{B}_n$, quindi $\mathcal{B}_n = \mathcal{P}_n\mathcal{V}_n$ e $\mathcal{P}_n \cap \mathcal{V}_n = \{id\}$

Osservazione: $\begin{array}{ccccc} (12) \circ v_1 & & \neq & v_1 \circ (12) & \\ {\color{red}1} & {\color{red}2} & & {\color{red}1} & {\color{red}2} \\ & \downarrow & & & \downarrow \\ {\color{red}2} & {\color{green}1} & & {\color{green}2} & {\color{red}1} \end{array}$

Quindi $\mathcal{B}_n$ non è prodotto diretto di $\mathcal{P}_n$ e $\mathcal{V}_n$.
$\mathcal{P}_n$ non è normale in $\mathcal{B}_n$ perché $(v_1 \circ (12) \circ v_1)({\color{red}1}, {\color{red}2}) \mapsto ({\color{green}2}, {\color{green}1}) \notin \mathcal{P}_n \Rightarrow \mathcal{P}_n \neg \trianglelefteq \mathcal{B}_n$

Definisco un omomorfismo $d : \mathcal{B}_n \to \mathcal{P}_n$ che dimentica i colori
d è un omomorfismo: $d(g_1 \cdot g_2) = d(g_1) \circ d(g_2)$ e $Ker(d) = \mathcal{V}_n$.
In particolare $\mathcal{V}_n \trianglelefteq \mathcal{B}_n$ e ${}^{\mathcal{B}_n}/_{\mathcal{V}_n} \simeq \mathcal{P}_n$ per TFO, quindi $\mathcal{B}_n = \mathcal{P}_n \ltimes \mathcal{V}_n$

Osservazione: $\mathcal{B}_n$ è il gruppo dei movimenti rigidi di R^n che fissa un cubo di dimensione $[-1, 1]^n \in \mathbb{R}^n$

Definizione di Gruppo dei Movimenti Rigidi di una Retta: È l'insieme
$\tilde{\mathscr{A}}_1 = \{\text{Movimenti Rigidi } f : \mathbb{R} \to \mathbb{R} \text{ tali che } f(\mathbb{Z}) = \mathbb{Z}\}$. Questo è costituito da $\{t^n, n \in \mathbb{Z}\}$ tale che $(t^n)(x) = x + n$ e dalle simmetrie $\{s_n, n \in \mathbb{Z}\}$ tale che $s(x) = -x$, $s_2(x) = -x + 2$ eccetera. Si può osservare che se n è pari è una simmetria rispetto ad un elemento di $\mathbb{Z}$, mentre se n è dispari è un elemento di $\frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}$.

Teorema: Sia G un gruppo e sia $H \leq G, N \trianglelefteq G, N \subseteq H$, allora:

1. $N \trianglelefteq H$
2. ${}^{H}/_{N} \leq {}^{G}/_{N}$
3. $H \trianglelefteq G \Leftrightarrow {}^{H}/_{N} \trianglelefteq {}^{G}/_{N}$
   Dimostrazione:
   1) Se $N \trianglelefteq G, gN = Ng, \forall g \in G$ e quindi a maggior ragione $gN = Ng, \forall g \in H \leq G \Rightarrow N \trianglelefteq H$
   2) Intanto ${}^{H}/_{N} \leq \subseteq {}^{G}/_{N} \Rightarrow \{gN, g \in H\} \subseteq \{gN, g \in G\}$ è sottogruppo perché $eN = N \in {}^{H}/_{N}$; se $h_1N, h_2N \in {}^{H}/_{N}$, cioè $h_1, h_2 \in H$, allora $h_1Nh_2H = h_1h_2N$ che appartiene ad ${}^{H}/_{N}$ perché $h_1, h_2 \in H$. Analogamente per gli inversi.
   3) $\Rightarrow$) $H \trianglelefteq G \Leftrightarrow \forall g \in G, \forall h \in H, \exists h' \in H \; t.c. \; ghg^{-1} = h'$
   $\Leftarrow$) ${}^{H}/_{N} \trianglelefteq {}^{G}/_{N} \Leftrightarrow \forall gN \in {}^{G}/_{N}, \forall gH \in {}^{H}/_{N}, \exists h'N \in {}^{H}/_{N}$ t.c. $gNhNg^{-1}N = h'N \Rightarrow (ghg^{-1})N = h'N \Leftrightarrow \exists n \in N$ t.c. $ghg^{-1}nh' \in H$ perché $N \subseteq H \Leftrightarrow ghg^{-1} \in H, \forall g \in G, \forall h \in H \Leftrightarrow H \trianglelefteq G$

Osservazione: Si può mostrare che $H \mapsto {}^{H}/_{N}$ è una biezione tra sottogruppi di G che contenga N e sottogruppi di ${}^{G}/_{N}$

Azioni

Definizione di Azione: Sia G un gruppo e X un insieme. Un'azione di G su X è un omomorfismo di $a : G \to Sym(X) = \{\text{Biezioni } X \to X\}$. Inoltre si ha che $\mathcal{O}(x) = \{g.x, g \in G\} \subseteq X$

Osservazione: In altre parole, un'azione di G su X è il dato (Elemento di X) per ogni $g \in G$ di una biezione di $a(g) : X \to X$, in modo tale che $a(g_1, g_2) = a(g_1)a(g_2) \in G$

Notazione: Quando è chiaro chi sia a, spesso si scrive $g.x$ invece di $a(g)(x)$

Esempi:
1) Quando abbiamo mostrato che $\sigma \in \mathfrak{S}_n$, non può essere sia pari sia dispari, abbiamo definito un'azione di $G = \mathfrak{S}_n$ e $X = \mathbb{K}[x_1, \dots, x_n] = \{\text{Polinomi in } n \text{ variabili}\}$: $\forall \sigma \in \mathfrak{S}_n, a(\sigma) : \mathbb{K}[x_1, \dots, x_n] \to [x_1, \dots, x_n], p(x_1, \dots, x_n) \mapsto p(x_{\sigma(1)}, \dots, x_{\sigma(n)})$
2) Parlando del simplesso abbiamo considerato un'azione di $\mathfrak{S}$ su $X = \{e_1, \dots, e_n\}$ data da $a(\sigma)(e_i) = e_{\sigma(i)}$ e quindi un'azione di $\mathfrak{S}$ su $\mathbb{K}^n$: $a(\sigma)(x_1, \dots, x_n) = (x_{\sigma(1)}, \dots, x_{\sigma(n)})$
3) Sia P_n un poligono regolare con n lati e $\mathfrak{D}_n$ il gruppo diedrale $\mathfrak{D}_n = \{\text{Movimenti rigidi del piano che fissano } P_n\}$ e siano $X = \{\text{Vertici di } P_n\}$. Abbiamo osservato che $\mathfrak{D}_n$ agisca su X e questo da un omomorfismo $a : \mathfrak{D} \to Sym(X) \simeq \mathfrak{S}_n$ (l'isomorfismo è dato numerando i vertici del poligono). Inoltre è iniettivo.
4) Abbiamo osservato che $\mathfrak{D}_6$ agisce $X = \{\text{Simmetrie rispetto ai vertici del poligono}\}$, ovvero ho un omomorfismo $\mathfrak{D}_6 \to Sym(X) \simeq \mathfrak{S}_3$
5) Nella dimostrazione del teorema di Cayley abbiamo definito $\forall g \in G, mg : G \to G, h \mapsto gh$. Osserviamo che $mg \in Sym(G) : h \mapsto gh$. Quindi $M : G \to Sym(G), g \mapsto mg$, $mg_1mg_2 = mg_1g_2$ è un'azione, cioè G agisce su G per moltiplicazione a sinistra.

6) Sia $H \leq G$, G agisce per moltiplicazione a sinistra sull'insieme delle classi laterali, cioè
$\overline{mg}: \ ^G/_H \to \ ^G/_H, kH \mapsto gkH \Rightarrow \overline{mg} \in Sym(^G/_H)$
7) Un gruppo G agisce su sé stesso per coniugio, cioè $\forall g \in G, C_g : G \to G, h \mapsto ghg^{-1}$, ho $C_g \in Aut(G) \leq Sym(G)$ e $C_{g_1} \circ C_{g_2} = C_{g_1 g_2} \Rightarrow C : G \to Sym(G), g \mapsto C_g$ è un omomorfismo, cioè ho un'azione
8) Se $H \leq G$, allora $\forall g \in G, C_g(H) = \{ghg^{-1}, h \in H\}$ è sottogruppo di G, quindi G agisce per coniugio su $X = \{\text{Sottogruppi di } G\}$

Definizione di Orbita: Data un'azione di G su X, per ogni $x \in X$, definisco Orbita di x, $\mathcal{O}(x) = \{g.x, g \in G\} = \{a(g)(x), g \in G\}$ Dico che l'orbita è Transitiva se G è composto da una sola orbita, ossia $\forall x, y \in X, \exists g \in G\ t.c.\ g.x = y$

Definizione di Stabilizzatore: Si chiama Stabilizzatore di x l'insieme $Stab_x = \{g \in G\ t.c.\ g.x = x\}$

Osservazione:

1. Le orbite danno una partizione di X, cioè "appartenere ad una stessa orbita" è una relazione di equivalenza
2. $\forall x \in X, Stab_x \leq G$

Esempio:
1) $G = \mathfrak{S}_3, X = \mathbb{K}[x_1, x_2, x_3], p(x_1, x_2, x_3) = x_1^2 + x_2 x_3$
$Stab_p = \{id, (23)\}$. Infatti:
$(13)p(x_1, x_2, x_3) = x_3^2 + x_2 x_1 = x_3^2 + x_1 x_2 = (132)p(x_1, x_2, x_3)$
$(12)p(x_1, x_2, x_3) = x_2^2 + x_1 x_3 = x_2^2 + x_3 x_1 = (123)p(x_1, x_2, x_3)$
$(id)p(x_1, x_2, x_3) = x_1^2 + x_2 x_3 = x_1^2 + x_3 x_2 = (23)p(x_1, x_2, x_3)$
Quindi $o_p = \{x_1^2 + x_2 x_3, x_2^2 + x_3 x_1, x_3^2 + x_1 x_2\}$
2) G agisce su G, per moltiplicazione a sinistra di $x \in G$. $o(x) = G$ perché $\forall y \in G, \exists g = yx^{-1}$ t.c. $g.x = yx^{-1}x = y$.
L'azione è transitiva $Stab_x = \{e\}$ per la legge di cancellazione: $g.x = x \Leftrightarrow x = e$
3) G agisce su G per coniugio, orbite=classi di coniugio, $Stab_x = \{g \in G\ t.c.\ C_g(x) \Leftrightarrow gxg^{-1} = x\} = \{g \in G, gx = xg\}$

Definizione di Centralizzatore: È l'insieme $Cen(x) = \{g \in G\ t.c.\ C_g(x) \Leftrightarrow gxg^{-1} = x\} = \{g \in G, gx = xg\}$

Osservazione: $Z(G) = \bigcap_{x \in G} (Cen(x))$

Teorema delle Orbite: Gli insiemi $o(x)$ e $^G/_{Stab_x}$ sono in biezione. Di conseguenza, se l'azione ha r orbite e $x_1, \dots, x_r$ è un insieme di rappresentanti delle orbite, allora $|X| = \sum_{i=1}^{r} [G : Stab_x]$

Dimostrazione
Definiamo un'applicazione $F : \begin{matrix} o(x) & \to & ^G/_{Stab_x} \\ gx & \mapsto & gStab_x \end{matrix}$, dove $gStab_x$ sono le classi laterali di g.
È ben definita se $g_1.x = g_2.x$ per qualche $g_1, g_2 \in G$, allora $g_2^{-1}g_1.x = e.x = x \Leftrightarrow g_2^{-1}g_1 \in Stab_x \Leftrightarrow g_1 Stab_x = g_2 Stab_x$
F è suriettiva per definizione
F è iniettiva perché se $g_1 Stab_x = g_2 Stab_x$ allora $g_2 = g_1 h, h \in Stab_x$ e dunque $g_2.x = g_1 h.x \Leftrightarrow g_1 \underbrace{hx}_{\in Stab_x} = g_1.x$

Poiché F è in biezione, $|\mathcal{O}(x)| = |\ ^G/_{Stab_x}| = [G : Stab_x]$ e poiché le orbite formano una partizione, $|X| = \sum_{i=1}^{r} |\mathcal{O}(x)|$

Definizione di Orbita Banale: Si dice che un'orbita $\mathcal{O}(x)$ è banale se $|\mathcal{O}(x)| = 1$, cioè se $\mathcal{O}(x) = \{x\}$

Osservazione: Considero l'azione di G su G per coniugio. Dunque le orbite sono le classi di coniugio e lo stabilizzante di X è $Cen(x)$ ($\Rightarrow Stab_x = Cen(x)$)

Osservazione: L'orbita $\mathcal{O}(x)$ di x è banale $\Leftrightarrow gxg^{-1} = x, \forall g \in G \Leftrightarrow gx = xg, \forall g \in G \Leftrightarrow x \in Z(G)$

Corollario (Formala delle Classi): Sia s il numero di classi di coniugio non banali e siano $g_1, \dots, g_a$ rappresentanti di tali classi. Allora $|G| = |Z(G)| + \sum_{i=1}^{r} [G : Cen(x)]$
Dimostrazione:
È la formula di prima, tenuto conto delle osservazioni precedenti.

Proposizione: Sia G un gruppo di Cardinalità p^m, dove p è primo e $m \geq 1$. Allora $Z(G)$ non può essere banale, $Z(G) \neq \{e\} \Rightarrow p|\ |Z(G)|$
Dimostrazione:

Per la formula delle classi, $|Z(G)| = |G| - \sum_{i=1}^{r}[G : Cen(x)]$. Poiché $Cen(g) \leq G, |Cen(g)| = p^a, a \leq m$. Se fosse $a = m$, avrei che $Cen(g) = G \Rightarrow g \in Z(G)$, assurdo perché tutti gli elementi del centro eran già a sinistra, quindi $a < m \Rightarrow p$ divide ogni addendo $\Rightarrow p||Z(G)|$

Proposizione: Sia G un gruppo di cardinalità p^2 (con p primo), allora g è commutativo.
Dimostrazione:
Per Lagrange $|Z(G)| = 1 \vee p \vee p^2$ ma non può essere 1 per la preposizione precedente, quindi $p \vee p^2$.
Supponiamo per assurdo che $|Z(G)| = p \Rightarrow \exists g_i \in G, g \notin Z(G)$. Allora $Cen(g_i)$ deve contenere sia g_i che $Z(G)$ e dunque ha almeno $p+1$ elementi. Ma allora per Lagrange $Cen(g_i)$ ha p^2 elementi $\Rightarrow$ quindi $Z(G)$ ha p^2 elementi $\Rightarrow G$ è commutativo.

Lemma: Dato $n \in \mathbb{N}, n \geq 1$ e dato un primo p, definiamo $mp(n) = \{max\ r \text{ t.c. } p^r|n\}$, cioè $n = p^r a, p \neg|a$, ossia $p \neg|\binom{n}{p^r}$
Esempio:
$n = 240, p = 2, mp(240) = 4$ e $\binom{240}{16} = \frac{240 \cdot 239 \cdot \ldots \cdot 225}{16 \cdot 15 \cdot \ldots 2 \cdot 1}$
Dimostrazione:
$\binom{n}{p^m} = \frac{p^m a \cdot (p^m a - 1) \cdot \ldots}{p^m \cdot (p^m - 1) \cdot \ldots} = a \prod_{i=1}^{p^m - 1} \frac{p^m a - 1}{p^m - i}$, adesso basta dimostrare che la frazione fattorizzata è divisibile per p.
In effetti se $i = p^s j$ con $p \neg|j$ e $j < m$ e $s < m$ (questo perché $i < p^m$), quindi
$\frac{p^m a - i}{p^m - i} = \frac{p^m a - p^s j}{p^m - p^s j} = \frac{p^s}{p^s} \frac{p^{m-s} a - j}{p^{m-s} - j} = \frac{p^{m-s} a - j}{p^{m-s} - j}$ che non è divisibile per p

Primo Teorema di Sylow: Sia G un gruppo e p un primo e sia $m = mp(|G|)$. Allora esiste un sottogruppo di G di cardinalità p^m detto sottogruppo di Sylow.
Dimostrazione:
Sia X l'insieme di tutti i sottoinsiemi di G di cardinalità m. Per la legge di cancellazione, se $X_0 \in X$, allora anche $gX_0 = \{gh, h \in X_0\} \in X \Rightarrow g$ agisce su X per moltiplicazione a sinistra.
Sempre per la legge di cancellazione, $\forall X_0 \in X, |Stab_{X_0}| \leq p^m$
Poiché se $g \in Stab_{X_0}, h \in X_0, gh \in X_0$ e se $g_1 \neq g_2 \Rightarrow g_1 h \neq g_2 h$. Osserviamo che $|X| = \binom{|G|}{p^n}$ e quindi per il lemma precedente, $p \nmid |X| = \sum_{i=1}^{r}[G : Stab_{X_i}]$
Dunque $\exists X_i \in X$ t.c. $p \neg|[G : Stab_{X_i}]$ e quindi $p^m|\ |Stab_X|$. Ma per quanto abbiamo visto prima. ossia che $|Stab_{X_0}| \leq p^m$ si ha che $|Stab_{X_i}| = p^m$

Esempio:
$G = GL(d, \mathbb{Z}_{/p})$, con p primo e $U = \{M \in G \mid M \text{ è triangolare superiore con tutti 1 sulla diagonale}\}$.
Vediamo che U è un p-sottogruppo di Sylow di G.
$M \in G \Leftrightarrow$ Le sue colonne formano una base di $(\mathbb{Z}_{/p})^d$. $|G| = (p^d - 1)(p^d - p)(p^d - p^2) \cdot \ldots \cdot (p^d - p^{d-1})$
Quindi $m_p(|G|) = 0 + 1 + 2 + \ldots + (d-1)$
Se $M \in U$, $M = \begin{pmatrix} 1 & * & \ldots & \ldots & * \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & * \\ 0 & \ldots & \ldots & 0 & 1 \end{pmatrix}$, allora $|U| = 1 \cdot p \cdot p^2 \cdot \ldots \cdot p^{d-1} \Rightarrow m_p(|U|) = 0 + 1 + 2 + (d-1)$

Osservazione: Abbiamo visto con il corollario del Teorema di Lagrange che se $g \in G$, allora $o(g)$ divide $|G|$, ma non vale il viceversa:

Esempio:
$|\mathscr{A}_4| = 12$ e $6|12$, ma $\mathscr{A}_4$ non ha sottogruppi di ordine 6

Però per i divisori primi di $|G|$ vale il viceversa.

Teorema di Cauchy: Sia p, un numero tale che p divida $|G|$, allora $\exists$ un elemento g tale che $o(g) = p$
Dimostrazione:
Lo verifico come il corollario del primo Teorema di Sylow.
Se $|G| = p^m a$ con $p \neg|a$, allora $\exists H \leq G$, con $|H| = p^m$. Sia $x \in H$ con $x \neq e \Rightarrow$ per Lagrange $o(x) = p^e$, dove $e = \{1, \ldots, m\}$ allora $g = x^{p^{e-1}} \Rightarrow g^p = (x^{p^{e-1}})^p = g^{p^d} = 1 \Rightarrow o(g) = p$

Lemma: Sia H un gruppo con $|H| = p^m$ che agisce su di un insieme X e sia X^H l'insieme dei punti fissi
$X^H = \{x \in X \mid hx = x, \forall h \in H\}$, allora $|X| \equiv |X^H| \quad (p)$
Dimostrazione:
Sia $x \in X$ tale che $Stab_x \neq H$ ($\Leftrightarrow x \in X \setminus X^H$), allora $|\mathcal{O}_x| = {}^{|H|}/_{|Stab_x|}$ è multiplo di p
Quindi, poiché le orbite formano una partizione di $|X| = |X^H| + \text{Multipli di p}$

Secondo Teorema di Sylow: Siano H, K due p-sottogruppi di Sylow di G, allora H e K sono coniugati (che siano $\exists g \in G$ t.c. $K = gHg^{-1}$)
Dimostrazione:
Sia $X = {}^G/_K$ e considerare l'azione di H su X per moltiplicazione a sinistra. Per il lemma appena dimostrato $[G : K] = |X| \equiv |X^H|$ modulo p, e quindi poiché $p \neg | [G : K] = a$, p non divide $|X^H| \Rightarrow X^H \neq \varnothing$.
In altre parole $\exists gK \in X^H$ per qualche $g \in G$
$hgK = gK, \forall h \in H$ (dalla definizione di X^H) $\Rightarrow g^{-1}hgK = K \Rightarrow g^{-1}Hg \subseteq K$.
Poiché $|g^{-1}Hg| = |H| = |K|$ e questo implica che $g^{-1}Hg = K$

Definizione di Normalizzatore: Sia $H \leq G$, con G un gruppo. Si chiama Normalizzatore di H in G e indicato con $N_G(H) = \{g \in G \mid gH = Hg\}$. Inoltre $H \trianglelefteq N_G(H)$

Terzo Teorema di Sylow: Sia $|G| = p^m a$ con $p \neg | a$ e sia $n_p =$ numero di $p-$Sylow di G, allora:

1. $n_p | a$
2. $n_p \equiv 1 \quad (p)$
   Dimostrazione:
   1) Sia X l'insieme di tutti i sottogruppi di Sylow di G. Per il primo Teorema di Sylow, X non è vuoto. Sia quindi $H \in X$, per il Secondo Teorema di Sylow, $n_p = |X| = |\mathcal{O}_x| = \frac{|G|}{|Stab_H|}$, dove $Stab_H = \{g \in G \mid gHg^{-1} = H\} = N_G(H)$ e $H \leq N_G(H)$. Per Lagrange si ha che $|H|$ divide $|Stab_H|$, quindi n_p divide $\frac{|G|}{|H|} = a$
   2) Considero l'azione di H su X e sia X^H l'insieme dei Punti Fissi. Se $K \in X^H$, cioè K è un $p-$sottogruppo di Sylow e $hKH^{-1}, \forall h \in H \Rightarrow H \leq N_G(K)$. Per il secondo Teorema di Sylow applicato a $N_G(K)$, H e K sono coniugati in $N_G(K)$, ma $K \trianglelefteq N_G(K) \Rightarrow K = H$. Quindi $X^H = \{H\}$ e per il lemma $|X| \equiv |X^H| \equiv 1 \quad (p)$

Osservazione: A volte le condizioni 1) e 2) implicano che $n_p = 1$. In questo caso l'unico $p-$sottogruppo di Sylow deve essere normale!

Esercizio:
Dimostrare che se $|G| = 15$, allora è ciclico
Soluzione:
Per il Terzo Teorema di Sylow $p = 3$, $n_3 \neg | 5 \wedge n_3 \equiv 1 \;\; (3) \Rightarrow n_3 = 1$.
Allo stesso modo si ottiene che $n_5 = 1$
Quindi $\exists ! K \leq G$ tale che $|H| = 3$ e $\exists ! K \leq G$ tale che $|K| = 5$
Visto che devo considerarli con i loro coniugati, $H \trianglelefteq G$ r $K \trianglelefteq G$
Si sa che $H \cap K < H, K$ e quindi per Lagrange si ottiene che $H \cap K = \{e\}$ e poiché
$3 \cdot 5 = 15 \Rightarrow HK = G \Rightarrow G = H \times K$
ma $H \simeq \mathbb{Z}_{/3}$ e $K \simeq \mathbb{Z}_{/5}$, quindi $G \simeq \mathbb{Z}_{/3} \times \mathbb{Z}_{/5} \simeq \mathbb{Z}_{/15}$ per il teorema Cinese del Resto.
Si può vedere come con 7 *non si avrebbe avuto lo stesso risultato in quanto* $7 \equiv 1 \;\; (3)$