Algebra

Marco Casu

Contents

1 Insiemi e Relazioni

Sappiamo già che un insieme non è altro di una collezione di oggetti distinti.

$$A = \{1, 2, 3, 4, 5\}$$

Ricapitoliamo le proprietà basiche degli insiemi :

- **Intersezione** - $A \cap B \to \{x | x \in A \wedge x \in B\}$
- **Unione** - $A \cup B \to \{x | x \in A \vee x \in B\}$
- **Sottoinsieme** - $A \subseteq B \to \{x \in A \implies x \in B\}$
- **Insieme complementare** - $A^c_{\text{in B}} \to \{x \in B | x \notin A\}$

1.1 Proprietà fondamentali degli insiemi

Elenchiamo le già note proprietà degli insiemi :

- **Associativa** - $(A \cap B) \cap C = (C \cap B) \cap A$ oppure $(A \cup B) \cup C = (C \cup B) \cup A$
- **De Morgan** - Se $A, B \subseteq C$ allora $(A \cap B)^c = A^c \cup B^c$ oppure $(A \cup B)^c = A^c \cap B^c$
- **Distributiva** - $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ oppure $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$

Un insieme particolare associato ad un dato insieme A è **l'insieme delle parti** di A, è l'insieme di tutti i possibili sotto-insiemi di A e si indica con :

$$\mathcal{P}(A) = \{B | B \subseteq A\} \tag{1}$$

Introduciamo adesso il concetto di **prodotto cartesiano** su due insiemi A e B, esso non è altro che l'insieme di tutte le coppie ordinate dove il primo elemento appartiene ad A ed il secondo elemento a B :

$$A \times B = \{(a, b) | a \in A, b \in B\} \tag{2}$$

1.2 Le Relazioni

Una relazione ρ da un insieme A ad un insieme B, è un sotto-insieme del prodotto cartesiano $A \times B$.

$$\rho \subseteq A \times B, \text{ se } (a, b) \in \rho \text{ si scrive } a\rho b \tag{3}$$

Il dominio di tale relazione ρ risulta essere :

$$\mathcal{D}(\rho) = \{a \in A | \exists b \in B \text{ per il quale risulti } a\rho b\} \tag{4}$$

La sua immagine :

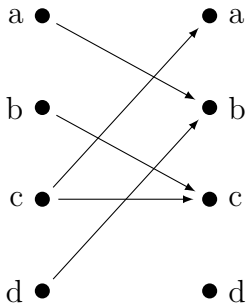
$$\Im(\rho) = \{b \in B | \exists a \in A \text{ per il quale risulti } a\rho b\} \tag{5}$$

Per una relazione ρ, se il suo dominio risulta essere tutto A, e $\forall a \in A \exists$ un unico $b \in B | a\rho b$, tale ρ è anche una **funzione**.
Esempio di relazione :
sia $A = \{a, b, c, d\}$, è definita la relazione $\rho \subseteq A \times A = \{(a, b), (b, c), (c, c), (c, a), (d, b)\}$.

Abbiamo due modi per poter visualizzare una relazione, un formato tabellare, ed un formato con nodi e collegamenti fra gli elementi della relazione. Per la relazione ρ appena enunciata si ha la seguente rappresentazione tabellare dove si inserisce un 1 nel punto in cui le due coordinate sono in relazione fra loro :

d	0	0	0	0
c	0	1	1	0
b	1	0	0	1
a	0	0	1	0
	a	b	c	d

Vediamone adesso una rappresentazione con nodi e collegamenti :



Essendo le relazioni degli insiemi, possiamo considerare le operazioni di unione ed intersezione anche per le relazioni. Esista per ogni relazione, anche la sua **relazione inversa**, se ρ è definita da A a B, esisterà ρ^{-1} definita da B a A.

$$\rho^{-1} = \{(b,a) \in B \times A | a\rho b\} \text{ quindi } a\rho b \implies b\rho^{-1}a \tag{6}$$

Se la relazione ρ è una funzione, non è detto che la sua relazione inversa sia una funzione anch'essa, prendiamo ad esempio la relazione $\rho \subset \mathbb{R} \times \mathbb{R} = \{(x, x^2) \forall a \in \mathbb{R}\}$, che non è altro che la funzione di una variabile reale $f(x) = x^2$. Tale funzione, per $x = -a$ ed $x = a$, ha sempre $f(x) = a^2$, per due valori appartenti al dominio ha la stessa immagine, la sua funzione inversa avrebbe quindi un punto che mappa due immagini.

Una relazione nota su insieme A è la **relazione identità**, definita : $\Delta_A = \{(a,a) \in A \times A\}$.

1.3 Relazioni di Equivalenza

Una relazione ρ definita su un insieme A, quindi $\rho \subseteq A \times A$, è detta **relazione di equivalenza** se soddisfa i seguenti requisiti :

- ρ è **riflessiva**, ossia è vero che : $a\rho a \forall a \in A$
- ρ è **simmetrica**, ossia è vero che se esiste $a\rho a'$ allora esiste $a'\rho a$
- ρ è **transitiva**, se esistono $a\rho a'$ e $a'\rho a''$, allora esiste $a\rho a''$

Un esempio di relazione di equivalenza è la relazione di *avere la stessa età* su un insieme di studenti, difatti soddisfa tutti e 3 i requisiti :

- è **riflessiva** perchè ognuno ha la stessa età di se stesso.
- è **simmetrica** perchè se tizio ha la stessa età di caio, caio ha la stessa età di tizio.
- è **transitiva** perchè se tizio ha la stessa età di caio e caio ha la stessa età di sempronio, tizio ha la stessa età di sempronio.

Un esempio di relazione **non** di equivalenza è la relazione di *genitorialità*, ad esempio non è simmetrica, perchè se tizio è padre di caio, caio non è assolutamente padre di tizio.

1.4 Le Classi di Equivalenza

Sia ρ una relazione di equivalenza definita su A, si definisce **classe di equivalenza** di un elemento $a \in A$, e si denota con $[a]$, l'insieme di tutti gli elementi di A che sono equivalenti (ossia in relazione di equivalenza) ad a, ossia

$$[a] = \{b \in A | b\rho a\} \tag{7}$$

Ad esempio, su una relazione di *avere la stessa età*, in ogni classe di equivalenza ci sono tutte le persone che hanno la stessa età : ogni classe può essere quindi un etichetta con il numero corrispondente all'età.
Esempio esteso :
Si prenda in considerazione il seguente insieme di persone :

$$A = \{\text{Valentino,Marco,Luca,Alessandro,Davide}\}$$

Ognuno ha i seguenti anni :

- Valentino - 20
- Marco - 19
- Luca - 20
- Alessandro - 19
- Davide - 19

La relazione di *avere la stessa età* su A è definita come :
$\rho = \{(Valentino, Luca), (Luca, Luca), (Marco, Alessandro), (Alessandro, Davide)...ecc\}$
La classe di equivalenza $[Marco] = \{Marco, Alessandro, Davide\}$ definisce tutti gli elementi in relazione con $Marco$, e rappresenta tutte le persone di età uguale a 19.

Sia A un insieme sulla quale è definita una relazione di equivalenza, l'insieme A/a è detto **insieme quoziente**, ed è l'insieme che contiene tutte le classi di equivalenza della relazione definita su A.

$$A/a = \{[a], a \in A\} \tag{8}$$

Vediamo adesso un **importante proprietà** delle classi di equivalenza :

Teorema 1

$$[a] = [b] \iff a\rho b \tag{9}$$

Dimostrazione 1 *Ovviamente* $b \in [b]$ *perchè* $b\rho b$*, essendo*
$[a] = [b] \implies b \in [a] \implies b\rho a \implies a\rho b$*, Analogamente, se* $a\rho b$*, se esiste*
$c \in [a] \implies c\rho a \implies c\rho b \implies c \in [b] \implies [a] \subseteq [b]$.
se esiste $c \in [b] \implies c\rho b \implies c\rho a \implies c \in [a] \implies [b] \subseteq [a]$*. Essendo* $[b] \subseteq [a]$ *e* $[a] \subseteq [b]$*, per forza di cose* $[a] = [b]$.

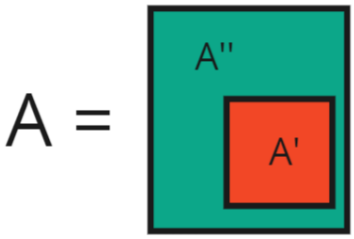
■

1.4.1 Le Partizioni

Dicesi **partizione** di un insieme A una *collezione di parti o sotto-insiemi* A_α non vuoti di A tali che **l'unione** di tutti i sotto-insiemi sia A, ossia, tali collezioni *ricoprono* A.

$$\bigcup_\alpha A_\alpha = A \tag{10}$$

Ciò significa che $A_\alpha \cap A_\beta \neq \varnothing \implies A_\alpha = A_\beta$, in un linguaggio meno formale, tutte le partizioni di un insieme A, non condividono nessun elemento di A. Nell'immagine seguente, A' e A'' sono partizioni di A.



Proposizione 1 *Sia ρ una relazione di equivalenza su A, le classi di equivalenza di ρ sono partizioni di A.*

Dimostrazione:
Ricoprono totalmente A, essendo $a\rho a \forall a \in A$, ogni a appartiene alla sua classe di equivalenza. Inoltre le classi di equivalenza, o coincidono o sono disgiunte.

Proposizione 2 *Ogni partizione di un insieme A determina su A una relazione di equivalenza, per la quale i sotto insiemi della partizione sono le classi di equivalenza.*

Dimostrazione:
Se indichiamo con B_α i sotto-insiemi della partizione A_α su A, è ovvio che :

$$a\rho b \implies \exists B_\alpha | a, b \in B_\alpha \tag{11}$$

Una relazione di equivalenza definisce a sua volta delle classi di equivalenza, che definiscono a loro volta delle partizioni.

1.5 Relazioni di Ordine Parziale

Introduciamo adesso un'altro gruppo di relazioni, ma prima necessitiamo della definizione di **relazione antisimmetrica** :

Sia ρ una relazione, essa si dice **antisimmetrica** se è vero che $a\rho b$ e $b\rho a \implies a = b$ (12)

Detto ciò, possiamo definire una *relazione di ordine* parziale se essa è :

- Riflessiva
- Transitiva
- Antisimmetrica

Esempio 1 - Sia X un insieme, e sia $\mathcal{P}(X)$ l'insieme delle sue parti, definiamo la relazione sugli elementi di $\mathcal{P}(X)$ nel seguente modo $\rho = \{\{A, B\}$ con $A, B \in \mathcal{P}(X)$ se $A \subseteq B\}$, quindi $A\rho B \iff A \subseteq B$, è chiaro che tale relazione soddisfa i 3 requisiti, è quindi di ordine parziale.

Esempio 2 - Prendiamo come relazione la divisibilità in $\mathbb{N}^* = \mathbb{N}\backslash\{0\}$, siano $a, b \in \mathbb{N}^*$ vale che $a\rho b \iff a|b$, dove $a|b$ significa *a divide b*, ossia che $\exists x \in \mathbb{N}^*$ tale che $b = a \cdot x$. Tale relazione è di ordine parziale dato che è riflessiva ($a = 1 \cdot a$ quindi $a\rho a$), è transitiva (dato che se a è divisibile per b e b è divisibile per c, è ovvio che a sia divisibile per c), e risulta essere anche antisimmetrica, dato che :

$$\begin{cases} a\rho b \\ b\rho a \end{cases} \implies \begin{cases} b = ax \\ a = by \end{cases} \implies a = (ax)y \implies xy = 1 \tag{13}$$

Quando si ha una relazione di ordine parziale, gli elementi di tale relazione godono della proprietà di poter essere rappresentati graficamente in un determinato modo, ma prima di enunciare tale rappresentazione, necessitiamo di una definizione.

Teorema 2 *Sia ρ una relazione d'ordine parziale su un insieme A, presi $a, b \in A$, diciamo che a* ***è coperto*** *da b e scriveremo*

$$a \preccurlyeq b \tag{14}$$

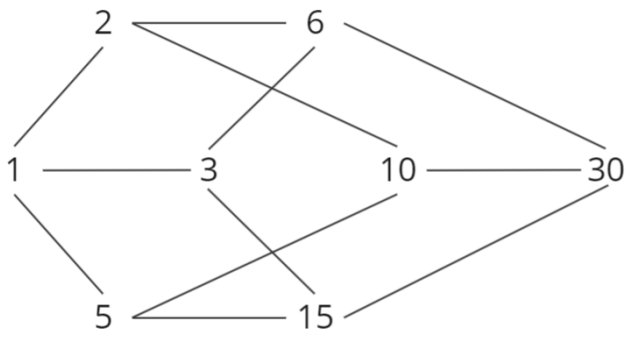
se $a\rho b$ e non esiste nessun elemento c tale che $a\rho c$ e $c\rho b$.

Ad esempio, prendiamo l'insieme $A = \{1, 2, 3, 5, 6.10, 15, 30\}$, ossia dei numeri naturali che dividono 30. Risulta chiaro come :

- $2! \preccurlyeq 30$ 30 non è il primo valore che si fa dividere da 2, ci sono valori prima di 30 per il quale 2 è divisore.
- $2! \preccurlyeq 3$ dato che 2 e 3 non sono nemmeno in relazione.
- $2 \preccurlyeq 6$ perchè 6 è il primo numero che 2 può dividere.

Stabilito ciò, possiamo *rappresentare graficamente* una relazione di ordine parziale su un insieme finito tramite il **diagramma di Hasse**, disegnando tutti gli elementi dell'insieme, collegandoli con una fraccia ogni dove un elemento *copre* un altro.

preso $A = \{1, 2, 3, 5, 6.10, 15, 30\}$ e la relazione di divisibilità prima enunciata, si ha



1.6 I Numeri Naturali

Dalle scuole elementari siamo abituati a lavorare e fare operazioni con i numeri naturali, in questa sezione ne daremo una definizione assiomatica in termini di *fondamenti della matematica*. È importante in questo momento non considerare assolutamente il concetto di numeri naturali che ci è ben chiaro, e cercare di leggere il seguente paragrafo da un punto di vista puramente logico, dando nulla per scontato.

1.6.1 La Terna di Peano

Introduciamo prima quella che è un'astrazione dei numeri naturali, ossia la **terna di Peano**.

$$(\mathbb{N}, \sigma, 0) \tag{15}$$

Si indica in questo caso con $\mathbb{N}$ un insieme di elementi, non i numeri naturali alla quale siamo abituati, con σ invece si indica una funzione $\sigma : \mathbb{N} \to \mathbb{N}$, e dato ogni elemento $n \in \mathbb{N}$, l'elemento $\sigma(n)$ si dice *successivo* di n. Su tale terna, sono definiti 3 fondamentali assiomi :

- $\mathbb{N}_1$ - σ è una funzione iniettiva.
- $\mathbb{N}_2$ - $0 \notin \Im(\sigma)$, 0 non è contenuto nell'immagine di σ.
- $\mathbb{N}_3$ (*Principio di induzione matematica*) - Se $U \subseteq \mathbb{N}$, ed è vero che :
  - $0 \in U$
  - $k \in U \implies \sigma(k) \in U$

  Allora $U = \mathbb{N}$

  Dimostrazione
  Considero $U = \{0\} \cup \{n | \exists n' \text{ tale che } \sigma(n') = n\}$ quindi $k \in U \implies \exists k' | k = \sigma(k')$ allora risulta ovvio che $\sigma(k) = \sigma(\sigma(k')) \in U \implies U = \mathbb{N}$.

1.6.2 Definizione Formale

Dati tali assiomi adesso procesiamo nel riconnetterci con l'insieme dei numeri naturali da noi conosciuti, enunciandone le proprietà elementari secondo la terna di Peano.
Sia $(\mathbb{N}, \sigma, 0)$ una terna di Peano, presi $n, m \in \mathbb{N}$, dirò che $n \leq m \iff m = \sigma(\sigma(\sigma(...n)))$, ossia che n è minore o uguale di m se m è uguale a σ applicato su n un certo numero di volte.

Proposizione - Questo stabilisce una relazione di ordine totale.

Adesso definiamo le operazioni elementari che conosciamo sui numeri naturali, ossia di somma e prodotto.
Definiamo la **somma** come operazione su un insieme $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, ossia che associa ad ogni coppia di elementi di $\mathbb{N}$, un elemento di $\mathbb{N}$.

$$n, m \in \mathbb{N} \text{ si definisce somma } n \times m \to n + m \tag{16}$$

La somma è definita in tal modo :

- (i) $0 + b = b$

- (ii) $\sigma(a) + b = \sigma(a + b)$

  Osservazione - $\sigma(0) + b = \sigma(0 + b) = \sigma(b)$, Se poniamo $\sigma(0) = 1$, allora vediamo che $\sigma(b) = b + 1$.

Definamo adesso il **prodotto**, sempre come un operazione $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ avente le seguenti proprietà :

- (i) $0 \cdot b = 0 \forall b \in \mathbb{N}$
- (ii) $\sigma(a) \cdot b = a \cdot b + b$

  Si può dire che gli assiomi di Peano caratterizzano i numeri naturali. Quello che si deve accettare senza dimostrazione, è l'esistenza di un insieme $\mathbb{N}$ *verificante gli assiomi di Peano.*

2 I Numeri Interi

Nell'insieme $\mathbb{N}$, non ci è permesso risolvere $x + 1 = 0$. In questo capitolo partiremo dai numeri naturali per costruirne un estensione in grado di rappresentare gli interi. Partendo dal prodotto cartesiano $\mathbb{N} \times \mathbb{N}$, costruiamo una relazione del tipo :

$$(n, m) \sim (n', m') \iff n + m' = m + n' \tag{17}$$

In linguaggio meno formale, una coppia $(0, a)$ è in relazione con tutte le coppie n, m, per cui $n - m = -a$, ed una coppia $(a, 0)$ è in relazione con tutte le coppie n, m, per cui $n - m = a$. *Esempio :*

$$(5, 6) \sim (0, 1) \iff 5 + 1 = 6 + 0$$
$$(8, 2) \sim (6, 0) \iff 8 + 0 = 2 + 6$$

Si nota facilmente come tale relazaione sia di equivalenza, possiamo quindi definire delle classi di equivalenza che ripartiscono l'insieme $\mathbb{N} \times \mathbb{N}$ in classi $[(n, m)]$. Scegliamo come *rappresentanti* delle classi di equivalenza gli elementi che prevedono uno dei due elementi uguale a *zero*, ogni classe sarà rappresentabile con uno dei seguenti rappresentanti distinti :

$$(0, 0)$$
$$(1, 0), (2, 0), (3, 0)..., (n, 0)...$$
$$(0, 1), (0, 2), (0, 3)..., (0, n)...$$

Abbiamo detto che ogni classe $[(a, 0)]$ contiene tutti gli elementi (n, m) per cui $n - m = a$, ad esempio si noti come :

$$[(5,0)] = \{(10,5),(35,30),(1434,1429)...\}$$

Analogamente :

$$[(0,3)] = \{(5,8),(1,4),(22,25)...\}$$

Poniamo per **definizione** :

$$\mathbb{Z} = {}^{\mathbb{N} \times \mathbb{N}}/_{\sim} \tag{18}$$

Ossia l'insieme $\mathbb{Z}$ è l'insieme quoziente[1] di $\mathbb{N} \times \mathbb{N}$ sulla relazione $\sim$ precedentemente definita. Possiamo inoltre decomporre $\mathbb{Z}$ nei seguenti sotto-insiemi :

$$\mathbb{Z} = \mathbb{Z}^+ \cup \{0\} \cup \mathbb{Z}^-$$

Dove (com'è di facile intuizione) si ha :

$$\begin{aligned} &\mathbb{Z}^+ = \{[(n,0)] | n \in \mathbb{N}\backslash\{0\}\} \\ &0 = [(0,0)] \\ &\mathbb{Z}^- = \{[(0,n)] | n \in \mathbb{N}\backslash\{0\}\} \end{aligned}$$

Gli elementi di $\mathbb{Z}^+$ saranno denominati **interi positivi** mentre quelli di $\mathbb{Z}^-$ **interi negativi**, l'insieme $\mathbb{Z}$ è un *estensione* di $\mathbb{N}$, dato che contiene al suo interno $\mathbb{Z}^+ \cup \{0\}$ che è identificabile come $\mathbb{N}$ tramite l'applicazione iniettiva da $\mathbb{N}$ in $\mathbb{Z}$ che associa ad ogni naturale n la classe $[(n,0)]$. Definiamo adesso su $\mathbb{Z}$ le operazioni elementari di somma e prodotto :

Somma :

$$[(n,m)] + [(n',m')] = [(n+n', m+m')]$$

Esempio 1 :

$$[(5,0)] + [(0,9)] = [(5,9)] = [(0,4)]$$

Prodotto :

$$[(n,m)] \cdot [(n',m')] = [(n \cdot n' + m \cdot m', n' \cdot m + n \cdot m')]$$

Esempio 2 :

$$[(7,0)] \cdot [(0,2)] = [(7 \cdot 0 + 0 \cdot 2, 0 \cdot 0 + 7 \cdot 2)] = [(0,14)]$$

Da ora in poi indicheremo gli elementi di $\mathbb{Z}$ in tal modo :

$$[(n,0)] = n \qquad [(0,0)] = 0 \qquad [(0,n)] = -n$$

Riprendendo gli esempi di prima, è chiaro come adesso siano definite le operazioni elementari che siamo abituati ad utilizzare fin dalle elementari.

$$\begin{aligned} &\textit{Esempio 1} \quad \to 5 + (-9) = -4 \\ &\textit{Esempio 2} \quad \to 7 \cdot (-2) = -14 \end{aligned}$$

Osservazioni :

$$[(n,0)] + [(0,n)] = [(n+0, 0+n)] = [(n,n)] \sim [(0,0)] \implies n + (-n) = 0$$

In $\mathbb{Z}$ ci sono due importanti elementi, $[(0,0)] = 0$ e $[(1,0)] = 1$, dati tali elementi e le operazioni precedentemente definite, diciamo che $\mathbb{Z}$ è una **struttura algebrica**.

[1] l'insieme di tutte le classi di equivalenza.

2.1 Divisibilità in $\mathbb{Z}$

Teorema Fondamentale : Presi due numeri $a, b \in \mathbb{Z}$, con $b \neq 0$, esistono e sono unici due numeri $q, r \in \mathbb{Z}$ tale che :

$$a = bq + r \text{ dove } 0 \leq r < |b|$$

Dove a è detto *dividendo*, b è detto *divisore*, q è detto *quoziente* ed r è detto *resto*.

Dimostrazione :
(*Esistenza*) Consideriamo un numero intero $b \geq 1$ e l'insieme $S = \{a - bx \geq 0, x \in \mathbb{Z}\}$, si ha che $S \neq \emptyset$ perchè, ponendo ad esempio $x = -|a|$, si verifica $a + b|a| \geq 0$. Per *principio del buon ordinamento*, essendo S sottoinsieme di $\mathbb{N}$, S ha un minimo, che denoteremo r. Quindi $r \in S \implies r = a - bq$ con $q \in \mathbb{Z}$. Segue che $a = bq + r$, e tale coppia q, r è unica dato che r essendo un minimo, è unico. Si dimostra facilmente $0 \leq r < |b|$, sicuramente $0 \leq r$ dato che $r \in S$, poniamo per assurdo che $r \geq |b|$, quindi $r - b \geq 0$. Dato che prima si è scritto $r = a - bq$, ora abbiamo $r - b = a - bq - b$, che possiamo riscrivere come $a - b(q + 1)$, che rientra nella forma $a - bx$ definita inizialmente nell'insieme S. Ciò vuol dire che $r - b \in S$, ovviamente $r > r - b$, ma r è il minimo di S quindi è **assurdo** che $r - b$ sia in S, per questo $r < |b|$.

Definizione : presi $a, b \in \mathbb{Z}$ si dice che a *divide* b, e si scrive $a|b$, se esiste $c \in \mathbb{Z}$ tale che $b = ac$.
Osservazioni :

- 1) ogni $a \in \mathbb{Z}$ ha sempre i divisori *ovvi*, ossia ± 1 e $\pm a$.
- 2) $\forall a \in \mathbb{Z}, a|0$.
- 3) $0|a \iff a = 0$
- 4) $a|1 \iff a = \pm 1$
- 5.1) se $a|b$ e $a|c$, allora $\forall x, \forall y, a|bx + cy$, si dimostra facilmente :

$$\begin{cases} a|b \implies b = at \\ a|c \implies c = as \end{cases} \implies bx + cy = atx + asy = a(tx + sy) \implies a|bx + xy \qquad (19)$$

- 5.2) se $\forall x, \forall y, a|bx + cy$, allora $a|b$ e $a|c$.

2.2 Il Massimo Comun Divisore

Definizione : Siano $a, b \neq 0, 0 \in \mathbb{Z}$, $d \geq 1 \in \mathbb{Z}$ si dice **massimo comun divisore** di (a, b) se:

- i) $d|a$ e $d|b$
- ii) se $d'|a$ e $d'|b$ allora $d'|d$

Il massimo comun divisore esiste $\forall a, b \neq 0, 0 \in \mathbb{Z}$ ed è *unico*.
Dimostrazione :
(*Esistenza*) Vogliamo dimostrare che $MCD(a, b)$ esiste. Sia
$S = \{ax + by > 0, \forall x, y \in \mathbb{Z}\} \subseteq \mathbb{N}\backslash\{0\}$ un insieme, ovviamente non vuoto, essendo

sotto-insieme dei numeri naturali vale il principio del buon ordinamento, quindi esiste un minimo in S, che denotiamo $d = ax_0 + by_0$. Vogliamo provare che $MCD(a,b) = d$, per la (5.2) basta dimostrare che $d|ax + by\ \forall x, y$, prendo $ax + by$ e lo divido per d, vale ovviamente : $ax + by = d \cdot q + r$ con $0 \leq r < |d|$. Ci basta ora dimostrare che $r = 0$. Supponiamo per *assurdo* che $r > 0$, ciò vorrebbe dire che, essendo $d = ax_0 + by_0$, ho che :

$$ax + by = (ax_0 + by_0) \cdot q + r \implies r = a(x - x_0 q) + b(y - y_0 q) \tag{20}$$

Essendo di tale forma, vuol dire che essendo maggiore di 0,$r \in S$. Si giunge ad una contraddizione, dato che r è strettamente minore di d, ma abbiamo definito d come il minimo di s, quindi è impossibile che $r > 0$. Essendo $r = 0$, si ha che $d|ax + by$, quindi $d|a$ e $d|b$, d è il massimo comun divisore. ■

Abbiamo visto che tale d può essere scritto nella forma $d = ax_0 + by_0$ per due coefficenti x_0, y_0. Tale forma è detta **identità di Bézout**, e *non è unica*. Vediamo alcune proposizioni:

- 1) se $a \neq 0$ e $a|b$, allora $MCD(a,b) = |a|$
- 2) $MCD(a, \pm a) = a$
- 3) $MCD(a, 0) = a$
- 4) $MCD(\pm 1, a) = 1$
- 5) Siano $a, b, c \in \mathbb{Z}$ tutti diversi da 0, vale che $MCD(ab, ac) = |a| \cdot MCD(b, c)$
- 6) $MCD(a,b) = d \implies MCD(\frac{a}{d}, \frac{b}{d}) = 1$

Definizione : Siano $a, b \neq 0$, se $MCD(a,b) = 1$, allora a e b si dicono *co-primi*. Se due numeri sono co-primi, allora $\exists r, s \in \mathbb{Z}$ t.c. $ar + bs = 1$.
Lemma di Euclide : se $a|bc$ e $MCD(a,b) = 1$ allora $a|c$.
Dimostrazione **:**
Abbiamo per ipotesi che $ar + bs = 1$, allora $c = c \cdot 1 = c \cdot (ar + bs)$, e per ipotesi essendo $a|bc$ vuol dire che $bc = ax$ per qualche x. allora $c = a(cr) + a(xs) = a(cr + xs) \implies a|c$. ■

Vediamo un importante *lemma*, sappiamo che se $a, b \in \mathbb{Z}$ con $b \neq 0$, si ha che $a = bq + r$ con $0 \leq r < |b|$. Si ha che $MCD(a,b) = MCD(b,r)$.
Dimostrazione **:**
Sia $d = MCD(a,b)$ e $d' = MCD(b,r)$. In generale, se $a|b$ e $b|a \implies a = \pm b$. Per tale osservazione, dobbiamo dimostrare che $d|d'$ e $d'|d$.

- Sappiamo che $d|a$ e $d|b$, quindi $d|a - bq \implies d|r$, essendo che $d|r$ e $d|b$, si ha che $d|d'$ perchè $d' = MCD(b,r)$.
- Sappiamo che $d'|d$ e $d'|r$, quindi $d'|bq + r \implies d'|a$, essendo che $d'|a$ e $d'|b$, si ha che $d'|d$ perchè $d = MCD(a,b)$.

■

2.2.1 L'Algoritmo Euclideo

Vediamo ora l'algoritmo per trovare il massimo comun divisore di due numeri a, b, per cui vale la condizione $a \geq b > 0$. Vediamo come si fa passo per passo.

- Passo 1) divido a per b, ed ottengo $a = bq_1 + r_1$. Se $r_1 \neq 0$, continuo.
- Passo 2) divido b per r_1, ed ottengo $b = r_1q_2 + r_2$. Se $r_2 \neq 0$, continuo.
- Passo 3) divido r_1 per r_2, ed ottengo $r_1 = r_2q_3 + r_3$. Se $r_3 \neq 0$, continuo.

Osservazione : Procedendo in tal modo, definiamo una successione di interi strettamente decrescente :

$$b > r_1 > r_2 > r_3...$$

Quindi, ad un certo punto, otterremo un resto pari a 0 :

- Passo n) divido r_{n-2} per r_{n-1}, ed ottengo $r_{n-2} = r_{n-2}q_n + r_n$. Se $r_n \neq 0$, continuo.
- Passo $n+1$) divido r_{n-1} per r_n, ed ottengo $r_{n-1} = r_nq_{n+1} + r_{n+1}$. A questo punto ho che $r_{n+1} = 0$

Ho trovato finalmente che $r_{n+1} = 0$, per lemma di Euclide, si ricordi che : $MCD(r_{n-1}, r_n) = MCD(r_n, r_{n+1}) \implies MCD(r_{n-1}, r_n) = MCD(r_n, 0) \implies MCD(r_{n-1}, r_n) = r_n$.
A questo punto risulta chiaro che :

$$MCD(a, b) = MCD(b, r_1) = MCD(r_1, r_2)..., = MCD(r_n, 0) = r_n \tag{21}$$

Quindi, $MCD(a, b)$ è uguale all'ultimo resto non nullo.

2.3 Equazioni Diofantee

Un *equazione diofantea* è un equazione della forma :

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

Dove si vogliono trovare delle soluzioni intere, ossia con $x, y \in \mathbb{Z}$. Tale equazione, ha soluzione intera **se e solo se** il massimo comun divisore fra a e b divide c.

$$\text{con } a, b, c \in \mathbb{Z}, \exists x, y \in \mathbb{Z} \text{ tale che } ax + by = c \iff MCD(a, b)|c$$

2.3.1 Risoluzione

Vediamo adesso passo-passo come si risolve un equazione di questo tipo:

- 1) Bisogna prima verificare che l'equazione sia risolvibile, si calcoli quindi $MCD(a, b) = d$, se esso divide c, l'equazione ammette soluzione.
- 2) Usare l'algoritmo euclideo2.2.1 per trovare un'identità di Bézout per d, esprimendolo nella forma $d = ax_0 + by_0$, utilizzeremo proprio tali coefficenti (x_0, y_0).
- 3) Moltiplicare (x_0, y_0) per $\frac{c}{d}$, ottenendo $(\tilde{x}, \tilde{y})$=$(\frac{c}{d} \cdot x_0, \frac{c}{d} \cdot y_0)$.
- 4) Per qualsiasi $k \in \mathbb{Z}$, le soluzioni dell'equazione diofantea sono della forma :

$$(\tilde{x} + k \cdot \frac{b}{d}, \tilde{y} - k \cdot \frac{a}{d})$$

Vediamo un *Esempio* di risoluzione, sia :

$$2x + 5y = 3$$

- Uso l'algoritmo di Euclide per trovare $MCD(5,2)$: $(1)5 = 2 \cdot 2 + 1$ $(2)2 = 2 \cdot 1 + 0$. Trovo quindi $MCD(5,2) = 1$.
- Tramite tale algoritmo, identifico anche la combinazione lineare $1 = (-2) \cdot 2 + (1) \cdot 5$.
- Moltiplico $(-2, 1)$ per 3, ottenendo $(-6, 3)$.
- Tutte le soluzioni sono : $(-6 + (k \cdot 5), 3 - (k \cdot 2))$, difatti, per $k = 1$ ho : $2(-6 + 5) + 5(3 - 2) = 3$.

2.4 Il Minimo Comune Multiplo

Il *minimo comune multiplo* fra due numeri a, b, che si indica con $mcm(a, b)$, è quel valore $h \geq 0$ tale che, $a|h$ e $b|h$, e se esiste h' tale che $a|h'$ e $b|h'$, allora $h|h'$. Ne seguono le seguenti osservazioni:

- 1) $mcm(a, 0) = 0$
- 2) $mcm(a, 1) = a$
- 3) $mcm(a.b) = 0 \implies a = o \vee b = 0$

Corollario : Se $a, b \in \mathbb{Z}$ e $a, b \neq 0$, allora $|ab| = MCD(a, b) \cdot mcm(a, b)$, quindi $mcm(a, b) = \dfrac{|ab|}{MCD(a, b)}$.

2.5 I Numeri Primi

Un intero $p \geq 2$ è detto *primo* se i suoi divisori sono esclusivamente ± 1 e $\pm p$. Quindi, segue la seguente osservazione : Se $p|xy$ e $p \nmid x \implies p|y$, è chiaro che p è primo se e solo se, se p divide un prodotto : $p|xy$, $x \neq \pm 1 \implies y = \pm 1$. La generalizzazione di elemento primo è la seguente :

Un elemento p di un anello 3.3 $(\mathbb{Z}, +, \cdot)$ è detto **irriducibile** se:

$$p = xy, x \notin \mathcal{U}(\mathbb{Z}) \implies y \in \mathcal{U}(\mathbb{Z})$$

Un qualsiasi dominio di integrità può presentare elementi primi o irriducibili, se $a \in A, +, \cdot)$ è primo, allora a è irriducibile (primo $\implies$ irriducibile). non è però vero il contrario, in generale, se un elemento è irriducibile, non è per forza primo (irriducibile $\nRightarrow$ primo). Nei numeri interi $\mathbb{Z}$, gli elementi irriducibili sono i numeri primi.

2.5.1 Teorema Fondamentale dell'Aritmetica

Se $n \geq 2$, $n \in \mathbb{N}$, tale n è un prodotto di numeri primi (può essere fattorizzato in numeri primi). Inoltre, tale fattorizzazione ha scrittura :

$$n = p_1^{h_1} \cdot p_2^{h_2} \cdot p_3^{h_3} ..., \cdot p_s^{h_s} \text{ con } h_i \geq 1 \text{ e } s \geq 1$$

Dove $p_1, p_2 ..., p_s$ sono s primi distinti, e tale scrittura è **unica** a meno dell'ordine dei fattori. Consegue che, preso un qualunque intero z diverso da zero e diverso da ± 1, ha scrittura :

$$z = \pm p_1^{h_1} \cdot p_2^{h_2} \cdot p_3^{h_3} ..., \cdot p_s^{h_s} \text{ con } h_i \geq 1 \text{ e } p_i \text{ irriducibili} > 1$$

Vediamo una proprietà, sia :

$$a = p_1^{h_1} \cdot p_2^{h_2} ..., \cdot p_s^{h_s}, \qquad\qquad b = p_1^{k_1} \cdot p_2^{k_2} ..., \cdot p_s^{k_s}$$

Ammettendo esponenti $h_i = 0$, è possibile scrivere le fattorizzazioni di due interi diversi con gli stessi identici primi distinti, "costringengo" ad essere presenti nella fattorizzazione anche primi che in realtà non apparirebbero, ma grazie ad esponente nullo diventano $p_i^0 = 1$. Date tali fattorizzazioni, si ha che :

$$MCD(a, b) = p_1^{m_1} \cdot p_2^{m_2} ..., \cdot p_s^{m_s}$$

$$mcm(a, b) = p_1^{M_1} \cdot p_2^{M_2} ..., \cdot p_s^{M_s}$$

Dove, per ogni i, tali esponenti sono : $m_i = \min\{h_i, k_i\}$ e $M_i = \max\{h_i, k_i\}$.
Proposizione : Esistono *infiniti* numeri primi. *Dimostrazione* : Supponiamo che i numeri primi siano in un numero finito : $p_1, p_2, p_3 ..., p_N$. Prendiamo adesso il numero $a = p_1 \cdot p_2 \cdot p_3 ... \cdot p_N + 1$. Tale numero è un intero positivo maggiore di 1, quindi, per il teorema fondamentale dell'aritmetica, deve per forza avere una fattorizzazione in numeri primi. Tuttavia, se esso viene diviso per ogni primo p_i dà come resto 1, questo è assurdo e ci assicura che i numeri primi sono necessariamente infiniti.
Corollario : $\forall p$ primo, $\nexists \sqrt{p} \in \mathbb{Q}$.

3 Strutture Algebriche Notevoli

Vediamo prima una definizione :

> Sia X un insieme, un **operazione binaria** in X è un *aapplicazione* $* : X \times X \to X$, ossia che ad ogni elemento del prodotto cartesiano $X \times X$ associa un elemento di X.

Ad esempio, l'operazione somma + nei numeri naturali è un operazione binaria. $(\mathbb{Z}, +)$ è un insieme con un'operazione binaria definita su di esso. Vediamo adesso alcune strutture algebriche notevoli e largamente studiate.

3.1 Definizione di Semigruppo

Il **semigruppo** è un insieme S dotato di un operazione $*$ verificante i seguenti punti :

- **1.1** - $*$ è **associativa**, ossia $(s * s') * s'' = s * s' * s''$.
- **1.2** - $\exists e \in S | e * s = s = s * e \forall s \in S$ dove tale e è detto **elemento neutro**.

Se dovesse accadere che $\forall s, s' \in S | s * s' = s' * s$ si dice che il semigruppo $S, *$ è anche **commutativo**.
Esempio 1 : Sia $S = \{f : X \to X\}$ l'insieme delle funzioni definite su un insieme X, l'operazione $\circ$ detta composizione è associativa, presenta l'elemento neutro (la funzione identità), ma non è commutativa, dato che $f \circ g \neq g \circ f$, quindi $(S, \circ)$ è un semigruppo non commutativo.

3.2 Definizione di Gruppo

Il **gruppo** è un insieme S dotato di un operazione $*$ verificante i punti del semigruppo, ma avendo una condizione aggiunta necessaria :

- **2.1** - $*$ è **associativa**, ossia $(s * s') * s'' = s * s' * s''$.
- **2.2** - $\exists e \in S | e * s = s = s * e \forall s \in S$ dove tale e è detto **elemento neutro**.
- **2.3** - $\forall s \in S \exists s' | s * s' = e = s' * s$ dove s' è detto **inverso** di s.

Esempio 1 : $(\mathbb{N}, +)$ non è un gruppo, ma $(\mathbb{Z}, +)$ si, dato che $\forall x \in \mathbb{Z} \exists -x | x + (-x) = 0$, ovviamente 0 è l'elemento neutro.
Esempio 2 : Sia X un insieme, l'insieme $S = \{f : X \to X$ biettiva$\}$ ossia di tutte le funzioni biettive su X, con l'operazione $\circ$ di composizione, è un gruppo, dato che
$\forall f \in S \exists f^{-1} | f \circ f^{-1} = d_x$, dove d_x è la funzione identità (l'elemento neutro).

È importante notare che per definizione, l'elemento neutro e, se esiste è unico. La **dimostrazione** è semplice : sia $\tilde{e}$ un'altro elemento neutro su $(S, *)$. dato che
$\forall s \in S | s * \tilde{e} = s = \tilde{e} * s \implies \tilde{e} * e = e = e * \tilde{e}$, ma dato che anche e è elemento neutro, $e * \tilde{e} = \tilde{e} = \tilde{e} * e$.

$$\begin{cases} e * \tilde{e} = \tilde{e} = \tilde{e} * e \\ \tilde{e} * e = e = e * \tilde{e} \end{cases} \implies \tilde{e} = e \textbf{ L'elemento neutro è unico.} \tag{22}$$

3.2.1 Il Gruppo Simmetrico S_n

Sia X un insieme ,abbiamo chiamato il gruppo di tutte le sue corrispondenze biunivoche $f : X \to X$ con il simbolo $(S(X), \circ)$, nel caso in cui X sia finito, con cardinalità $|X| = n$, si indicherà con S_n, e prende il nome di **gruppo simmetrico di grado** n. Tale gruppo non è commutativo, data l'operazione di composizione $\circ$. È facile notare come ogni elemento σ di S_n sia una permutazione di $X = \{1, 2, 3, 4..., n\}$, quindi la cardinalità sarà $|S_n| = n!$.

3.3 Definizione di Anello

L'anello $(A, \odot, *)$ è un insieme dotato di 2 operazioni con le seguenti proprietà :

- **3.1** - $(A, \odot)$ è un **gruppo commutativo**, dove O_A è l'elemento neutro.
- **3.2** - L'operazione $*$ è **associativa**.
- **3.3** - Riguardo le due operazioni, valgono le proprietà **distributive** :

$$(a \odot a') * b = (a * b) \odot (a' * b) \tag{23}$$

Per essere un anello, non è necessario che l'operazione $*$ sia commutativa, nel caso dovesse esserlo, l'anello si dice commutativo.
Un anello si dice **unitario** se $\exists u \in A | a * u = a = u * a \forall a \in A$, ossia, se è definito l'elemento neutro sull'operazione $*$.
Un anello commutativo, è detto **privo di divisori dello zero** se :

$$a * b = O_A \implies a = O_A \vee b = O_A \tag{24}$$

Dove si ricordi che O_A è l'elemento neutro definito su $(A, \odot)$.
Se un anello commutativo è privo di divisori dello zero, ed è unitario, si dice **dominio di integrità**.
L'insieme dei numeri interi $(\mathbb{Z}, +, \cdot, 0)$ è un *anello commutativo unitario* con unità 1, privo di divisori dello 0, detto quindi *dominio di integrità*.

Proprietà dell'anello

- **(1)** $\forall a \in A, a \cdot 0 = 0$ ciò si dimostra facilmente, infatti $a \cdot 0 = a \cdot 0 + 0$, ma essendo che $a \cdot 0 = a \cdot (0 + 0)$ si ha $a \cdot 0 + 0 = a \cdot (0 + 0)$, aggiungo ad entrambi i membri $-a \cdot 0$ ed ottengo $-a \cdot 0 + a \cdot 0 + 0 = -a \cdot 0 + a \cdot 0 + a \cdot 0 \implies 0 + 0 = a \cdot 0 + 0 \implies a \cdot 0 = 0$. ■
- **(2)** $a \cdot (-b) = -(-ab) = (-a) \cdot b$
- **(3)** $(-a) \cdot (-b) = ab$
- **(4)** $a \cdot (b - c) = (a \cdot b) - (a \cdot c)$

In ogni anello unitario (non necessariamente commutativo) $(A, +, \cdot)$ si definisce $\mathcal{U}(A) = \{a \in A | \exists a' | a \cdot a' = 1 = a' \cdot a\}$, ossia l'insieme degli elementi invertibili di A, ad esempio, nei numeri interi si ha $\mathcal{U}(\mathbb{Z}) = \{1, -1\}$. Si nota facilmente che l'insieme degli elementi invertibili è un gruppo. Vediamo ora un importante proprietà :

$$a, b \in \mathcal{U}(A) \implies a \cdot b \in \mathcal{U}(A)$$

Ossia, il prodotto di due elementi invertibili, è anche esso un elemento invertibile.
Dimostrazione:
Siano a' l'inverso moltiplicativo di a e b' l'inverso moltiplicativo di b, quindi $a, b, a', b' \in \mathcal{U}(A)$.
Ciò vuol dire che $a' \cdot b'$ è l'inverso moltiplicativo di $a \cdot b$, dato che
$(a' \cdot b') \cdot (a \cdot b) = b' \cdot (a' \cdot a) \cdot b = b' \cdot 1 \cdot b = b' \cdot b = 1$, è quindi dimostrato che essendo $a'b'$ l'inverso di ab, essi sono invertibili, per cui fanno parte di $\mathcal{U}(A)$. ■

Notazioni semplificate

Da questo punto in poi useremo le seguenti notazioni semplificate :

- **Gruppo** - $(S, \cdot, 1)$ dove "S" è l'insieme, "$\cdot$" l'operazione, ed "1" l'elemento neutro.
- **Gruppo Commutativo** - $(S, +, 0)$ dove "S" è l'insieme, "$+$" l'operazione, e "0" l'elemento neutro.
- **Anello** - $(A, +, \cdot, 0)$ dove "S" è l'insieme, "$+$" la prima operazione, per cui $(A, +)$ risulta un gruppo commutativo, "$\cdot$" la seconda operazione, e "0" l'elemento neutro. Se unitario, si usa "1" come simbolo per l'unità.

3.4 Definizione di Campo

Abbiamo visto che l'insieme degli invertibili di un anello è uguale a tutti quegli elementi, che moltiplicati per un altro elemento dell'insieme, detto *inverso*, sono uguali all'elemento neutro rispetto l'operazione di prodotto. Infatti in un anello, l'inverso esiste per tutti gli elementi rispetto l'operazione di somma (essendo un gruppo), ma non del prodotto.
Da qui possiamo dare la definizione di **campo**, che si denota con $\mathbb{K}, +, \cdot$, e non è altro che un *anello commutativo unitario* per cui vale la seguente proprietà :

$\forall k \in \mathbb{K}, k \neq 0, \exists k' | k \cdot k' = 1$ dove 1 è l'elemento neutro rispetto all'operazione "$\cdot$", e 0 è l'elemento neutro rispetto all'operazione "$+$".

Quindi un campo, è un anello commutativo unitario per cui esiste l'inverso di ogni elemento rispetto l'operazione di prodotto, difatti vale che $\mathcal{U}(\mathbb{K}) = \mathbb{K} \backslash \{0\}$. Due noti esempi di campo che conosciamo sono il campo dei numeri razionali $\mathbb{Q}$ ed il campo dei numeri reali $\mathbb{R}$.

4 L'Anello $\mathbb{Z}_n$

L'insieme dei numeri interi $\mathbb{Z}$ è il più semplice e chiaro esempio di anello. Vediamo adesso un anello commutativo unitario, **con divisori dello zero**, che non sia quindi dominio di integrità. Definiamo prima di tutto una relazione :

$$a \sim_n b \iff a - b \text{ è divisibile per } n \tag{25}$$

L'insieme $\mathbb{Z}_n \equiv {}^{\mathbb{Z}}/_{\sim_n}$ non è altro che l'insieme quoziente di tale relazione sui numeri interi. Ossia l'insieme delle sue classi di equivalenza. $\mathbb{Z}_n = \{[0], [1], [2]..., [n-1]\}$. Notiamo come la cardinalità di tale insieme sia proprio n, e che :

$$[-1] = [n-1] \text{ perchè } n - 1 \sim_n 1 \iff n - 1 - (-1) = n$$
$$[0] = [n] \text{ perchè } n \sim_n 0 \iff n - 0 = n$$
$$[1] = [n+1] \text{ perchè } n + 1 \sim_n 1 \iff n + 1 - 1 = n$$
$$[10] = [n+10] \text{ perchè } n + 10 \sim_n 10 \iff n + 10 - 10 = n$$

Su tale insieme sono definiti somma e prodotto (ben posti):

$$[k] + [h] = [k + h]$$
$$[k] \cdot [h] = [k \cdot h]$$

Ha un elemento neutro per la somma [0], ed uno per il prodotto [1]. L'anello è commutativo ed unitario, però possiede *divisori dello zero*, se prendo ad esempio $\mathbb{Z}_{12}$, nonostante $[3] \neq [4] \neq [0]$, risulta che $[3] \cdot [4] = [12] = [0]$ perchè $12 \sim_{12} 0 \iff 12 - 0 = 12$ e 12 è divisibile per 12. *Osservazione:* Se non si è in un dominio di integrità non è possibile

semplificare un equazione, si prenda $\mathbb{Z}_{10}$, sicuramente $[8] = [2][4]$ e $[8] = [28] = [7][4]$, quindi $[7][4] = [2][4]$, semplificando il $[4]$ otterrei $[7] = [2]$ che non è vero.

Notazione : Al posto di $\mathbb{Z}_n$ scriveremo (mod n), e se $a = b$ (mod n), potremmo anche scrivere $a \equiv b$ (mod n).

4.1 Equazioni in $\mathbb{Z}_n$: Congruenze Lineari

In questo paragrafo ci occuperemo di esplicare come si risolve un equazione detta *congruenza lineare*, del tipo :

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

Ossia, trovare un x_0 tale che $ax_0 \equiv b$ in $\mathbb{Z}_n$.
Proposizione : La congruenza lineare $ax \equiv b$ (mod n) ammette soluzioni **se e solo se** $MCD(a, n)|b$. La *Dimostrazione* è semplice, dato che risolvore una congruenza lineare equivale a risolvere un equazione diofantea2.3 del tipo:

$$ax + ny = b$$

Proposizione : Se x_0 è una soluzione di $ax \equiv b$ (mod n), *tutte* le soluzioni di tale congruenza saranno del tipo :

$$x_0 + h \cdot \frac{n}{MCD(a, n)} \text{ con } h \in \mathbb{Z}$$

Ma tale generalizzazione identifica infinite soluzioni congruenti fra loro, le soluzioni diverse (mod n) sono quindi esattamente $d = MCD(a, n)$.
Come accennato precedentemente, per risolvere una congruenza lineare $ax \equiv b$ (mod n), basta risolvere $ax + ny = b$, trovando : $(x_0 + h \cdot \frac{n}{MCD(a,n)}, y_0 + h \cdot \frac{a}{MCD(a,n)})$, e considerando la prima coordinata della coppia.

4.2 La funzione di Eulero

Il *Teorema di Eulero*, enucia che, se n è un intero positivo, ed a è co-primo rispetto ad n, allora è vero che :

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

Dove φ è la **funzione di Eulero**, che associa ad ogni n, il numero di tutti gli interi positivi minori di n, che sono co-primi con n. Ad *esempio* :

- $\varphi(20) = 8$ perchè i co-primi con 20 minori di esso sono : $1, 3, 7, 9, 11, 13, 17, 19$.
- $\varphi(6) = 2$ perchè i co-primi con 6 minori di esso sono : $1, 5$.

Ci occuperemo di capire come calcolare $\varphi(n)$ per ogni intero n della quale si conosca la *fattorizzazione*.

Proposizione : Sia $n = p_1^{h_1} \cdot p_2^{h_2} ... \cdot p_k^{h_k}$ la fattorizzazione in numeri primi di n, dove $\forall i \in \{1, 2..., k\}$, p_i è un numero primo distinto, risulta :

$$\varphi(n) = \varphi(p_1^{h_1}) \cdot \varphi(p_2^{h_2}) ..., \cdot \varphi(p_k^{h_k})$$

Con tale risultato, non rimane che calcolare il valore di φ sulle potenze dei numeri primi.

Proposizione : Se p è un numero primo, allora :

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

Tale risultato risulta quasi scontato, tutti i numeri co-primi con un numero primo, sono tutti i numeri minori di tale numero, dato che esso non condivide divisori con nessuno. Parlando di potenze, non sono co-primi con p^h, solo i multipli di p, che sono del tipo : $p \cdot i$. Ora per ogni n della quale si conosca la fattorizzazione, siamo in grado di calcolare la sua funzione di Eulero :

- $\varphi(72) = \varphi(2^3 \cdot 3^2) = \varphi(2^3)\varphi(3^2) = (2^3 - 2^2)(3^2 - 3) = (4)(6) = 24$
- $\varphi(8) = \varphi(2^3) = (2^3 - 2^2) = 4$

4.2.1 Gli Invertibili di $\mathbb{Z}_n$

Ricordiamo che $\mathbb{Z}_n$ ha la struttura di un anello commutativo con unità3.3, ha quindi un insieme di elementi invertibili. Vogliamo determinare la cardinalità di tale insieme $\mathcal{U}(\mathbb{Z}_n)$.

Proposizione : In $\mathbb{Z}_n$, gli unici elementi *invertibili* sono quelle classi a tali che $MCD(a, n) = 1$.
Ossia, tutti gli elementi co-primi con n, ed equivale a risolvere la congruenza :

$$ax \equiv 1 \pmod{n}$$

Tale congruenza ammette un unica soluzione, se e solo se $MCD(a, n) = 1$. Gli invertibili, sono esattamente $\varphi(n)$, quindi, se p è primo, tutti gli elementi di $\mathbb{Z}_p$ escluso lo 0 sono co-primi con p, quindi, ogni classe non nulla è invertibile : $|\mathcal{U}(\mathbb{Z}_p)| = \varphi(p) = p - 1$.
Ricordando che un campo è un anello commutativo con unità, per cui ogni elemento non nullo è invertibile, si arriva al seguente risultato :

Se p è un numero primo, allora l'anello $\mathbb{Z}_p$ è un *campo*.

4.2.2 Il Teorema di Eulero

Se $n \geq 2$, $a \in \mathbb{Z}$ e $MCD(a, n) = 1$, allora :

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

4.3 Sistemi di Congruenze e Teorema Cinese del Resto

Osserviamo il seguente *sistema* :

$$\begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \\ ... \\ a_s x \equiv b_s \pmod{n_s} \end{cases} \tag{26}$$

Si vuole trovare una soluzione intera che sia soluzione di tutte le equazioni del sistema. Il sistema per avere soluzione, deve avere ognuna delle sue equazioni risolvibili, quindi

$\forall i, j, i \neq j \implies MCD(a_i, n_i)|b_i$. Prima di vedere la soluzione di tale sistema, si consideri un altro sistema della forma :

$$\begin{cases} x \equiv c_1 \pmod{r_1} \\ x \equiv c_2 \pmod{r_2} \\ ... \\ x \equiv c_s \pmod{r_s} \end{cases} \quad i \neq j \implies MCD(r_i, r_j) = 1 \tag{27}$$

Dove ogni argomento del modulo, è coprimo con tutti gli altri. Tale sistema si dice di tipo *cinese*. Il *teorema cinese del resto* enuncia che, un sistema di questo tipo ammette soluzione ed è **unica** in (mod $r_1 \cdot r_2 ... \cdot r_s$).

Dimostrazione(e risoluzione) : Consideriamo il prodotto di tutti gli argomenti dei moduli, ossia $R = r_1 \cdot r_2 ... \cdot r_s$, e, per ogni k-esima equazione del sistema, si consideri $R_k = \dfrac{R}{r_k}$. Risulta ovvio che, essendo R un prodotto di numeri co-primi, $MCD(R_k, r_k) = 1$, quindi ogni congruenza lineare $R_k x \equiv c_k \pmod{r_k}$ ammette una soluzione unica (si ricordi che le soluzioni distinte di una congruenza lineare $ax \equiv b \pmod{n}$ sono in numero $MCD(a, n)$).
Consideriamo adesso, per ogni k-esima equazione del sistema, la sua soluzione $\tilde{x}_k$, che si trova risolvendo l'equazione diofantea (derivante dall'identità di Bézout) $R_k t_k + r_k g_k = 1$, una volta trovato il coefficente t_k, la soluzione è $\tilde{x}_k = t_k c_k$. Una volta trovate le soluzioni di ogni equazione, la soluzione generale del sistema sarà :

$$\tilde{x} = \sum_{i=1}^{s} \tilde{x}_i R_i$$

Quindi, $\forall i, \tilde{x} = c_i \pmod{r_i}$.

Torniamo adesso al caso generale, in cui si ha un sistema del tipo :

$$\begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \\ ... \\ a_s x \equiv b_s \pmod{n_s} \end{cases} \tag{28}$$

Se sono vere alcune supposizioni, ossia:

- Ogni equazione del sistema ammette soluzione, $\forall i, j | i \neq j \implies MCD(a_i, n_i)|b_i$.
- Gli argomenti dei moduli sono tutti co-primi fra loro, $\forall i, j | i \neq j \implies MCD(n_i, n_j) = 1$

Possiamo dividere ogni elemento di ogni equazione del sistema per il corrispettivo massimo comun divisore fra a_i e n_i:

$$d_i = MCD(a_i, n_i) \begin{cases} \frac{a_1}{d_1} x \equiv \frac{b_1}{d_1} \pmod{\frac{n_1}{d_1}} \\ \frac{a_2}{d_2} x \equiv \frac{b_2}{d_2} \pmod{\frac{n_2}{d_2}} \\ ... \\ \frac{a_s}{d_s} x \equiv \frac{b_s}{d_s} \pmod{\frac{n_s}{d_s}} \end{cases} \tag{29}$$

Adesso, si ha che $MCD(\frac{a_i}{d_i}, \frac{n_i}{d_i}) = 1$, quindi $\frac{a_i}{d_i}$ è *invertibile* in (mod $\frac{n_i}{d_i}$). Per ogni equazione del sistema, moltiplico tutto per l'inverso di $\frac{a_i}{d_i}$, ottenendo $x \equiv c_i \pmod{\frac{n_i}{d_i}}$, ottenendo un sistema di tipo cinese, per la quale conosciamo il metodo risolutivo :

$$d_i = MCD(a_i, n_i) \begin{cases} x \equiv c_1 \pmod{\frac{n_1}{d_1}} \\ x \equiv c_2 \pmod{\frac{n_2}{d_2}} \\ ... \\ x \equiv c_s \pmod{\frac{n_s}{d_s}} \end{cases} \tag{30}$$

4.3.1 Seconda Formulazione del Teorema Cinese del Resto

> In questa specifica sezione, si farà riferimento ad argomenti trattati nel capitolo 7, si invita quindi il lettore, a soffermarsi su questa sezione esclusivamente dopo aver trattato il capitolo sulla *Teoria degli Anelli*.

Appunto sulla notazione : con $[a]_n$ si definisce la classe di equivalenza di a in $\mathbb{Z}_n$.

Vediamo adesso una definizione differente del teorema cinese del resto, si prenda come esempio un sistema con due sole equazioni :

$$\begin{cases} x \equiv a \pmod{r} \\ x \equiv b \pmod{s} \end{cases} \quad MCD(r, s) = 1 \tag{31}$$

Consideriamo adesso *l'applicazione* $F : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$ definita nel seguente modo :

$$[x]_{rs} \to ([x]_r, [x]_s) \tag{32}$$

Ossia che ad ogni classe di equivalenza in $\mathbb{Z}_{rs}$, assegna la coppia delle due classi di equivalenza dello stesso intero, ma rispettivamente $\mathbb{Z}_r$ e $\mathbb{Z}_s$.
Ebbene, tale applicazione è ben definita, e vale che :

$$x \equiv x' \pmod{rs} \implies \begin{cases} x \equiv x' \pmod{r} \\ x \equiv x' \pmod{s} \end{cases} \tag{33}$$

Ossia, sia l'equazione a sinistra che il sistema a destra hanno la stessa identica soluzione.

Tale applicazione F è un **isomorfismo** di anelli.

Teorema :
Dato il seguente sistema di tipo cinese :

$$\begin{cases} x \equiv a \pmod{r} \\ x \equiv b \pmod{s} \end{cases} \quad MCD(r, s) = 1 \tag{34}$$

e date le seguenti condizioni :

- (1) L'applicazione $F : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$ è biettiva
- (2) $MCD(r, s) = 1$

- (3) Il sistema ha un'unica soluzione $\text{mod}(r \cdot s)$

Vale che :

$$(1) \iff (2) \iff (3)$$

Ossia che se una qualsiasi delle 3 condizioni è vera, anche le altre sono vere, si implicano a vicenda in maniera circolare.
Dimostrazione :
$\boxed{(2) \implies (1)}$ - Abbiamo come ipotesi le condizioni (2) e (3), supponiamo per assurdo che $MCD(r,s) = d > 1$, sia $mcm(r,s) = h$, per il teorema fondamentale dell'aritmetica, $MCD(r,s) \cdot mcm(r,s) = dh = rs$, quindi $h = \dfrac{rs}{d}$, è chiaro che $h \geq 1$, e che $h < rs$, quindi sicuramente $[h]_{rs} \neq [0]_{rs}$. d'altra parte però, $r|h$ e $s|h$, quindi $[h]_r = [0]_r$ e $[h]_s = [0]_s$, ma se consideriamo l'applicazione F, si ha che :

$$\begin{cases} F([0]_{rs}) = ([0]_r, [0]_s) \\ [0]_r = [h]_r \wedge [0]_s = [h]_s \implies ([0]_r, [0]_s) = ([h]_r, [h]_s) = F([h]_{rs}) \end{cases}$$

Ma abbiamo detto che $[h]_{rs} \neq [0]_{rs}$, quindi F non può essere iniettiva, ma ciò va contro la tesi iniziale, quindi necessariamente $MCD(r,s) = 1$.
$\boxed{(3) \implies (1)}$ - Per ipotesi, $\exists! x | x \equiv a \bmod(r) \wedge x \equiv b \bmod(s)$, quindi, è anche vero che per tale x vale : $x \equiv a \bmod(rs) \wedge x \equiv b \bmod(rs)$, se prendo allora $[x]_{rs}$ ho che $F([x]_{rs}) = ([x]_r, [x]_s) = ([a]_r, [b]_s)$, quindi F è suriettiva. Essendo per l'ipotesi (3) che la soluzione è unica, F è anche iniettiva. Inoltre come ulteriore rafforzante per la nostra tesi, si ha che $|\mathbb{Z}_r \times \mathbb{Z}_s| = |\mathbb{Z}_{rs}|$, Essendo la cardinalità degli insiemi la stessa, se l'applicazione F è iniettiva, è anche necessariamente suriettiva, quindi biettiva. ■
Conclusione - Tale teorema enuncia che avvolte la risoluzione di un'equazione congruenziale è equivalente alla risoluzione di un sistema, e viceversa, ad esempio, la soluzione dei due problemi è equivalente :

$$8x \equiv 3 \bmod(385) \iff \begin{cases} 8x \equiv 3 \bmod(5) \\ 8x \equiv 3 \bmod(7) \\ 8x \equiv 3 \bmod(11) \end{cases} \tag{35}$$

4.4 Piccolo Teorema di Fermat

Sia p un numero primo, vale che : $\forall a \in \mathbb{Z},\ a^p \equiv a \pmod p$

Dimostrazione : Si dimostra per induzione.

- Caso Base $a = 0$ - $0^p = 0$
- Passo Induttivo - Per ipotesi, $a^p \equiv a \pmod p$, prendiamo $a + 1$, si ha :

$$(a+1)^p = a^p + 1 \tag{36}$$

Ma $a^p \equiv a$ quindi $a^p + 1 \equiv a + 1 \implies (a+1)^p \equiv a^p + 1 \pmod p$. ■

5 I Numeri Razionali

Abbiamo definito i numeri naturali, che servono per la definizione degli interi, che useremo a loro volta per definire i **numeri razionali**. Prima però, dobbiamo stabilire una *relazione* su $\mathbb{Z} \times \mathbb{Z}\backslash\{0\}$, ossia sul prodotto cartesiano fra gli interi, e gli interi escluso l'elemento neutro rispetto la somma. Definiamo la relazione ρ in tal modo :

$$(a,b)\rho(c,d) \iff a \cdot d = b \cdot c \tag{37}$$

Ad esempio, $(2,1)\rho(4,2)$ perchè $2 \cdot 2 = 4 \cdot 1$, oppure $(3,2)\rho(6,4)$ perchè $3 \cdot 4 = 6 \cdot 2$. Definiamo l'insieme dei razionali come l'insieme quoziente del prodotto cartesiano fra gli interi, e gli interi escluso l'elemento neutro rispetto la somma, rispetto la relazione appena definita.

$$\mathbb{Q} = \left\{ {}^{\mathbb{Z} \times \mathbb{Z}\backslash\{0\}}/_{\rho} \right\}$$

Ossia l'insieme di tutte le classi di equivalenza. Denotiamo poi $0 := [(0,1)]$ e $1 := [(1,1)]$. Come abbiamo visto prima, $(2,1)\rho(4,2)$, quindi $[(2,1)] = [(4,2)]$. Come abbiamo detto in precedenza, $\mathbb{Q}$ è un campo. Definiamo quindi due operazioni, ossia la somma ed il prodotto.

- somma : $[(a,b)] + [(c,d)] = [(ad + bc, bd)]$
- prodotto : $[(a,b)] \cdot [(c,d)] = [(ac, bd)]$

Tali operazioni fra classi di equivalenza sono *ben poste*, ossia non dipendono dalla scelta dei rappresentanti delle classi. Difatti se $[(a,b)] = [(c,d)]$ e $[(a',b')] = [(c',d')]$, si avrà che $[(a,b)] + [(a',b')] = [(c,d)] + [(c',d')]$, ossia che
$(ab' + ba', bb')\rho(cd' + dc', dd') \implies (ab' + ba') \cdot dd' = bb' \cdot (cd' + dc')$.

Abbiamo quindi due operazioni con definiti elementi neutri, uno per la somma $0 := [(0,1)]$ ed uno per il prodotto $1 := [(1,1)]$, è un anello commutativo unitario, ed inoltre è un campo, dato che presi qualsiasi $[(a,b)]$ con $a \neq 0$ allora $[(a,b)] \cdot [(b,a)] = 1$, questo è di facile verifica dato che $[(a,b)] \cdot [(b,a)] = [(ab,ba)] = [(1,1)] = 1$ dato che $(ab,ba)\rho(1,1) \iff ab \cdot 1 = ba \cdot 1$, ed essendo il prodotto definito su $\mathbb{Z}$ commutativo, ciò risulta vero.

L'insieme $\mathbb{Z}$ si identifica come sotto-insieme di $\mathbb{Q}$, dato che c'è un'applicazione iniettiva φ che associa ad ogni intero, la sua classe in $\mathbb{Q}$. Per ogni intero a, si ha $\varphi(a) = [(a,1)]$. Inoltre, è compatibile con le operazioni di somma e prodotto, dato che:

$$\varphi(a+b) = \varphi(a) + \varphi(b) = [(a,1)] + [(b,1)] = [(a \cdot 1 + b \cdot 1, 1 \cdot 1)] = [(a+b,1)]$$

Si dice che $\mathbb{Z}$ è sotto-insieme di $\mathbb{Q}$, di fatti $\mathbb{Z}$ è in biezione con $\{[(a,1)] | a \in \mathbb{Z}\}$. L'inverso di $[(a,b)]$ è $[(b,a)]$. Possiamo usare una **notazione semplificata** e denotare ogni elemento:

$$[(a,b)] := \frac{a}{b}$$

Qui risultano chiare note tutte le proprietà e le operazioni fatte sui razionali che svolgiamo fin dalle elementari.

$[(3,2)] + [(9,4)] = [(3 \cdot 4 + 2 \cdot 9, 2 \cdot 4)]$ in notazione semplificata risulta $\frac{3}{2} + \frac{9}{4} = \frac{3 \cdot 4 + 2 \cdot 9}{2 \cdot 4} = \frac{12 + 18}{8} = \frac{30}{8} = \frac{15}{4}$ dato che $[(30,8)] = [(15,4)] \iff (30,8)\rho(15,4) \iff 30 \cdot 4 = 15 \cdot 8$

6 Il Campo dei Numeri Complessi

Un equazione del tipo $3x = 5$ non ha soluzione in $\mathbb{Z}$, si è appunto creata una sua estension $\mathbb{Q}$ che ammette la soluzione $x = \frac{5}{3}$. Un equazione del tipo $x^2 = 2$ non ha soluzione nei numeri razionali, ma la ha in quella dei numeri reali, ossia $x = \sqrt{2}$. Vediamo l'equazione $x^2 + 1 = 0$, è un equazione di secondo grado che non ammette nessuna soluzione reale, di fatto non esistono numeri reali, il quale quadrato equivale a -1. Esiste un estensione di $\mathbb{R}$, definita nel seguente modo.

6.1 Definizione

I **numeri complessi** sono una struttura di questo tipo : si consideri $\mathbb{R}^2 = \{(x, y)|x, y \in \mathbb{R}\}$, ossia tutte le coppie ordinate di numeri reali, ed introduciamo due operazioni :

- **Somma** - $(x, y) + (x', y') = (x + x', y + y')$
- **Prdototto** - $(x, y) \cdot (x', y') = (xx' - yy', xy' + yx')$

Si noti come l'elemento neutro additivo è $(0, 0)$ e l'elemento neutro moltiplicativo $(1, 0)$. Ogni elemento ha un inverso, presa la coppia $(x, y) \neq (0, 0)$ si ha :

$$(x, y)^{-1} = (\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2}) \tag{38}$$

Dimostrazione :

$$(x, y) \cdot (\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2}) = (x \cdot \frac{x}{x^2 + y^2} - y \cdot \frac{-y}{x^2 + y^2}, x \cdot \frac{-y}{x^2 + y^2} + y \cdot \frac{x}{x^2 + y^2}) = \tag{39}$$

$$= (\frac{x^2 + y^2}{x^2 + y^2}, \frac{-xy + xy}{x^2 + y^2}) = (1, 0) \quad \blacksquare \tag{40}$$

$(R^2, +, \cdot)$ è un **campo** noto come *campo dei numeri complessi* ed è denotato con $\mathbb{C}$. Esiste un applicazione iniettiva φ da $\mathbb{R}$ a $\mathbb{C}$ che associa $\varphi : x \to (x, 0)$. R è un *sotto-campo* di $\mathbb{C}$, dato che l'applicazione *conserva* le operazioni, i complessi sono quindi un estensione dei reali.

$$\varphi(x \cdot_{\mathbb{R}} x') = \varphi(x) \cdot_{\mathbb{C}} \varphi(x') \tag{41}$$

$$\varphi(x +_{\mathbb{R}} x') = \varphi(x) +_{\mathbb{C}} \varphi(x') \tag{42}$$

L'equazione iniziale $x^2 + 1 = 0$, che possiamo riscrivere $x^2 + (1, 0) = (0, 0)$, ammette soluzione in $\mathbb{C}$, ed è proprio $x = (0, 1)$, difatti :

$$(0, 1)^2 + (1, 0) = (0, 0) \implies (0, 1)(0, 1) + (1, 0) = (0, 0) \implies (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) + (1, 0) = (0, 0) \implies (-1, 0) + (1, 0) = (0, 0) \implies (-1 + 1, 0) = (0, 0) \implies (0, 0) = (0, 0) \checkmark$$

Denoteremo $(a, 0) \equiv a$ per ogni $a \in \mathbb{R}$. Notiamo come qualsiasi numero complesso della forma (a, b) può essere riscritto come $(a, 0) + (0, b)$, ma $(0, b) = (0, 1)(b, 0)$, quindi posso rappresentare ogni numero come $(a, 0) + (0, 1)(b, 0)$, ossia la somma di un reale con un altro reale moltiplicato per $(0, 1)$. Tale numero viene denotato con i, ed è detta **unità immaginaria**, possiamo quindi rappresentare ogni numero complesso nella seguente forma : $(a, b) \equiv a + ib$, con $i^2 = -1$.

6.2 Teorema Fondamentale dell'Algebra

Ogni equazione algebrica con coefficenti complessi (quindi in particolare reali) di grado n, ammette precisamente n soluzioni in $\mathbb{C}$ (contando le moltiplicità). Si dice che $\mathbb{C}$ è **algebricamente chiuso**.

7 Elementi di Teoria degli Anelli

7.1 Isomorfismi e Omomorfismi tra Anelli

Abbiamo visto precedentemente la definizione assiomatica di *Anello*, presentiamo ora un altra importante definizione :

Definizione 1 *Un **isomorfismo** φ tra due anelli $(R, +_R, \cdot_R)$ e $(R', +_{R'}, \cdot_{R'})$ è una corrispondenza biunivoca tra R e R' che conserva le operazioni, tale che*

$$\varphi(a +_R b) = \varphi(a) +_{R'} \varphi(b) \ \forall a, b \in R$$
$$\varphi(a \cdot_R b) = \varphi(a) \cdot_{R'} \varphi(b) \ \forall a, b \in R$$

Se i due anelli sono *isomorfi*, si scrive $R \backsimeq R'$. La relazione di isomorfismo è una relazione di equivalenza, e qualunque proprietà algebrica che vale in R, vale anche in R', e viceversa, godendo delle stesse proprietà, dal punti di vista algebrico sono *indistinguibili*, si considerano quindi uguali due anelli isomorfi.

Spesso fra due anelli, esiste un applicazione che ne conservi le operazioni, ma che non è biunivoca. Si da la seguente definizione:

Definizione 2 *Dati due anelli $(R, +_R, \cdot_R)$ e $(R', +_{R'}, \cdot_{R'})$, si chiama **omomorfismo** di R in R' ogni corrispondenza (non necessariamente biunivoca) φ da R ad R' tale che :*

$$\varphi(r_1 +_R r_2) = \varphi(r_1) +_{R'} \varphi(r_2) \ \forall r_1, r_2 \in R$$
$$\varphi(r_1 \cdot +_R r_2) = \varphi(r_1) \cdot_{R'} \varphi(r_2) \ \forall r_1, r_2 \in R$$

Se φ è un isomorfismo di due anelli $(A, +_A, \cdot_A)$ e $(B, +_B, \cdot_B)$, ovviamente l'unità viene mappata nell'unità : $\varphi(1_A) = 1_B$, la dimostrazione è semplice :

$$\begin{cases} \varphi(1_A) = \varphi(1_A \cdot_A 1_A) = \varphi(1_A) \cdot_B \varphi(1_A) \\ 1_B = (\varphi(1_A))^{-1} \cdot_B \varphi(1_A) = (\varphi(1_A))^{-1} \cdot_B \varphi(1_A) \cdot_B \varphi(1_A) \end{cases} \implies 1_B = 1_B \cdot_B \varphi(1_A) = \varphi(1_A)$$

7.1.1 Nucleo di un omomorfismo

Inoltre si definisce un **nucleo** di omomorfismo φ tra R e R', il sotto-insieme di R costituito da tutti gli elementi che hanno come immagine l'elemento neutro rispetto la somma (lo zero) di R', indicato con $0_{R'}$. Tale nucleo si indica con :

$$Ker\varphi = \{r \in R | \varphi(r) = 0_{R'}\} \tag{43}$$

Esempio :
Prendiamo l'ismorfismo $\varphi : \mathbb{Q} \to \mathbb{Q}$ definito come $\varphi(a) = a + (-2)$, avremo che $Ker\varphi = \{2\}$.

$Ker\varphi$ gode di un importante *proprietà*, moltiplicando un qualunque $a \in Ker\varphi$ per un qualunque $b \in R$, il risultato sarà sempre un elemento di $Ker\varphi$:

$$\text{siano } k \in Ker\varphi \text{ e } r \in R \text{ vale che } \varphi(k \cdot r) = \varphi(k) \cdot \varphi(r) = 0 \cdot \varphi(r) = 0 \tag{44}$$

7.1.2 Ideale di un Anello

Definiamo adesso cos'è un **ideale** :
Un *ideale destro* di un anello R, è un sotto-gruppo additivo I di R, tale che, $\forall a \in I$ e $\forall r \in R$, risulta che $ar \in I$.
Un *ideale sinistro* di un anello R, è un sotto-gruppo additivo I di R, tale che, $\forall a \in I$ e $\forall r \in R$, vale che $r \cdot a \in I$.
Se un ideale è sia sinistro che destro si dice *bilatero*, e si denota nel seguente modo :

$$I \trianglelefteq R \tag{45}$$

Per come l'abbiamo definito prima, è ovvio che il nucleo di un omomorfismo tra due anelli $Ker\varphi$ sia un ideale bilatero. Ogni anello R possiede due ideali detti *banali*, ossia $\{0\}$ e R.

$\{0\}$ è un ideale I di R perchè $\forall a \in R$, essendo 0 l'unico elemento di I, è ovvio che $a \cdot 0 = 0 \cdot a = 0 \in I$.

7.2 Prodotto Diretto di Anelli

Siano $(A, +_A, \cdot_A)$ e $(B, +_B, \cdot_B)$ due anelli commutativi unitari, vale che, il risultato del loro prodotto cartesiano, detto **prodotto diretto di anelli**, ha una *naturale struttura* di anello, e preserva le operazioni in tal modo :

$$\begin{gathered}\text{Siano } a, a' \in A \text{ e } b, b' \in B \\ \text{somma : } (a,b) + (a',b') = (a +_A a', b +_B b') \\ \text{prodotto : } (a,b) \cdot (a',b') = (a \cdot_A a', b \cdot_B b')\end{gathered}$$

Quindi $(A \times B, +, \cdot)$ è un anello. L'elemento neutro è $0_{A \wedge B} = (0_A, 0_B)$, ossia la coppia dei due elementi neutri rispettivamente per A e B.

8 Teoria dei Gruppi

In questo capitolo ci occuperemo di studiare le proprietà dei gruppi, ricordiamo la definizione : $(G, *)$ è un gruppo se $*$ è un operazione binaria tale che :

1. $*$ è associativa.
2. $\exists e | g * e = g = e * g$
3. $\forall g \in G \ \exists g' | g * g' = e = g' * g$

Abbiamo già visto che l'elemento neutro e è **unico** e si identifica con 1 oppure 1_G, l'inverso di un elemento g, si denota con g^{-1}.

8.1 Omomorfismo tra Gruppi

Siano $(G, *)$ e $(G', \cdot)$ due gruppi, un applicazione φ tra G e G' si dice **omomorfismo** se :

$$\varphi(a * b) = \varphi(a) \cdot \varphi(b) \text{ con } a, b \in G$$

Ossia se *conserva* l'operazione. Prima abbiamo parlato di gruppo simmetrico, esso stabilisce sempre un omomorfismo iniettivo *canonico* $\varphi : (X, *) \to (S(X), \circ)$. Se un omomorfismo è anche biunivoco, si dice **isomorofismo**.

8.2 Sottogruppi

Definizione : Sia $(G, *)$ un gruppo, e sia $S \subseteq G$, tale che $1_G \in S$, diremo che S è un *sottogruppo* di G, e scriveremo $S \leq (G, *)$ se l'operazione di G :

$$* : S \times S \to S$$

è ben definita su S, e risulta essere chiuso rispetto a $*$, inoltre $\forall s \in S \exists s^{-1} \in S$.

Proposizione : In definitiva, $S \subseteq G$ è un sottogruppo se

- $\forall s_1, s_2 \in S, s_1 * s_2 \in S$
- $\forall s \in S, \exists s^{-1} \in S$

da tali due affermazioni ne consegue che $1_G \in S$. Detto ciò, possiamo implicare dalle 3 affermazioni precedenti un *criterio*, che, se valido, conferma che S sia un sottogruppo :

$$(3)\ \forall s_1, s_2 \in S, s_1 * s_2^{-1} \in S$$

Dimostrazione : Se S è un sottogruppo, $1_G \in S$, quindi $1_G = s * s^{-1} \in S$, per la (3), prendendo $s_1 = 1_G$ ed $s_2 = s$, si ha che $1_G * s^{-1} = s^{-1} \in S$, infine, presi $s_1 = a$ ed $s_2 = b^{-1}$, si ha che $a * (b^{-1})^{-1} = a * b \in S$. Quindi (3) è condizione necessaria e sufficente per dimostrare che S è un sottogruppo di G. ■

Proposizione : L'immagine di un omomorfismo φ, ossia $Im(\varphi) = \{\varphi(g), \forall g \in G\}$, è un *sottogruppo.*
Dimostrazione : Siano $y_1, y_2 \in Im(\varphi)$, ciò implica che $y_1 * y_2^{-1} \in Im(\varphi)$, per ipotesi, $\exists g_1, g_2 | y_1 = \varphi(g_1) \wedge y_2 = \varphi(g_2)$. Si ha che $y_1 * y_2^{-1} = \varphi(g_1) * \varphi(g_2)^{-1}$, essendo φ un omomorfismo, tale scrittura è equivalente a $\varphi(g_1) * \varphi(g_2^{-1}) = \varphi(g_1 * g_2^{-1})$, quindi in definitiva $y_1 * y_2^{-1} = \varphi(g_1 * g_2^{-1})$. ■

Ogni omomorfismo è un sottogruppo.

Ogni gruppo ha sempre due *sottogruppi banali*, ossia il gruppo identità $(1_G, *)$ ed il gruppo stesso.

8.2.1 Esempi di Sottogruppi

Esempio 1 Si consideri il gruppo $(\mathbb{R}\backslash\{0\}, \cdot)$ ho che $(\mathbb{R}^{>0}, \cdot)$ è un suo sottogruppo, se prendo due qualsiasi $a, b \in \mathbb{R}^{>0}$, ho che $a \cdot b^{-1} \in \mathbb{R}^{>0}$.

Esempio 2 Si consideri $(\mathbb{Z}, +)$, e considero l'insieme $n\mathbb{Z} = \{nh, h \in \mathbb{Z}\}$, ossia tutti i multipli di n, si ha che $(n\mathbb{Z}, +)$ è un sottogruppo di $(\mathbb{Z}, +)$, infatti, presi due qualsiasi $nh_1, nh_2 \in n\mathbb{Z}$ ho che $nh_1 + nh_2^{-1} = nh_1 - nh_2 = n(h_1 - h_2) \in n\mathbb{Z}$.

Esempio 3 Considero il gruppo $(\mathbb{Z}_n, +)$, prendo un intero d tale che d divide n, ossia $n = kd$ per qualche k. Considero adesso l'insieme :

$$H_d := \{[d], [2d], [3d], [4d]..., [(k-1)d], [n]\}$$

Tale insieme H_d rispetto a $+$ è un sottogruppo di $(\mathbb{Z}_n, +)$, dato che presi due qualsiasi a, b, ho che $[ad] - [bd] = [ad - bd] = [(a-b)d] \in H_d$.

8.3 I Sottogruppi di $\mathbb{Z}$ e $\mathbb{Z}_n$

In questo paragrafo enunceremo e dimostreremo due proposizioni piuttosto importanti, che descrivono la totalità dei sottogruppi di due gruppi a noi molto noti.

Proposizione 1 : Se H è un sottogruppo di $(\mathbb{Z}, +)$, allora $\exists n | n\mathbb{Z} = H$.
Dimostrazione 1 : Per ipotesi $H \leq (\mathbb{Z}, +)$, quindi $H \cap \mathbb{N} \neq \emptyset$, perché se $a \in H$, allora anche $-a \in H$, quindi H contiene elementi positivi. Per principio del buon ordinamento, H ha un minimo (positivo), sia esso n. Siccome H è un gruppo, ogni multiplo di n è in H, vale a dire che $n\mathbb{Z} \subset H$.
Affermiamo che ogni elemento di H sia divisibile per n, questo perchè, per qualsiasi $a \in H$ si ha $a = qn + r$, ricordando che $0 \leq r < n$, ma n è il minimo positivo, quindi $r = 0$, allora ogni elemento è divisibile per n, ne concludiamo che $H \subset n\mathbb{Z}$.

$$\begin{cases} H \subset n\mathbb{Z} \\ n\mathbb{Z} \subset H \end{cases} \implies n\mathbb{Z} = H$$

■

tutti i sottogruppi di $\mathbb{Z}$ sono del tipo $n\mathbb{Z}$.

Proposizione 2 : Se H è un sottogruppo di $(\mathbb{Z}_n, +)$, allora $\exists d$ tale che d divide n, ossia $n = kd$, quindi $H = H_d := \{[d], [2d], [3d], [4d]..., [(k-1)d], [n]\}$.
Dimostrazione 2 : Consideriamo l'insieme $H' = \{a \in \mathbb{Z} | [a] \in H\}$, ovviamente, $[0] = [n] \in H$, quindi $0 \in H'$. Anche $n \in H'$, risulta chiaro che $H' \neq \emptyset$ ed è un sottogruppo di $\mathbb{Z}$. Siano $a, b \in H'$, essendo un sottogruppo, $a + b^{-1} = a - b \in H'$, ne consegue che $[a - b] \in H \iff a - b \in H'$, sapendo che $H' \leq (\mathbb{Z}, +)$, per la *proposizione 1* appena vista, $\exists d | d\mathbb{Z} = H'$, avendo già visto che $n \in H'$, sappiamo ora che n è un multiplo di d, quindi è chiara la struttura dell'insieme $H' = \{d, 2d, 3d, 4d..., n\}$, avendo detto all'inizio che $H' = \{a \in \mathbb{Z} | [a] \in H\}$, è ovvio che $H = H_d$. ■

tutti i sottogruppi di $\mathbb{Z}_n$ sono del tipo H_d.

Ad esempio, i sottogruppi di $(\mathbb{Z}_{12}, +)$ sono :

$$\{[0]\}, \mathbb{Z}_{12}, H_2, H_3, H_4, H_6$$

Essendo $n = kd$, la cardinalità di H_d è k. Se un gruppo ha cardinalità finita, la sua cardinalità identifica il suo **ordine**. Per i gruppi finiti, è possibile considerare la *tabella moltiplicativa* :

$*$	1	g_1	g_2	g_3	...	g_n
1	1+1					
g_1				$g_3 + g_1$		
g_2						
g_3			$g_2 + g_3$			
...						
g_n						$g_n + g_n$

8.4 Gruppo Ciclico e Classi Laterali

8.4.1 Gruppo Generato

Prima di parlare dell'argomento di tale paragrafo, introduciamo una notazione :

Sia $(G, *)$ un gruppo, preso $g \in G$ e $t \in \mathbb{Z}$, si ha la seguente notazione :

$$g^t = \begin{cases} 1_G \text{ se } t = 0 \\ g * g * g ... * g \text{ per } t\text{-volte se } t > 0 \\ g^{-1} * g^{-1} * g^{-1} ... * g^{-1} \text{ per } t\text{-volte se } t < 0 \end{cases}$$

Ne segue :

- $g^s * g^t = g^{s+t}$
- $g^{-t} = (g^{-1})^t = (g^t)^{-1}$

L'insieme $\{g^t, t \in \mathbb{Z}\}$ è un sotto-gruppo di G, dato che presi g^{t_1} e g^{t_2}, si ha che:

$$g^{t_1} * (g^{t_2})^{-1} = g^{t_1} * g^{-t_2} = g^{t_1 - t_2} \in \{g^t, t \in \mathbb{Z}\}$$

Questo sottogruppo ha simbolo $\langle g \rangle$ ed è denominato sottogruppo **generato** da g.

Definizione : Sia $(G, *)$ un gruppo ed $H \leq (G, *)$, H è detto sottogruppo **ciclico** se $\exists h \in H | H =< h >$, ed in generale, $(G, *)$ è un gruppo **ciclico** se $\exists g \in G | G =< g >$, ossia è generato da un suo elemento. Se $(G, *)$ è ciclico, allora è **commutativo**, dato che $g^s + g^t = g^{s+t} = g^t + g^s$.
Esempio : $(\mathbb{Z}, +)$ è un gruppo ciclico perché è generato dal numero 1, infatti, $\mathbb{Z} = \langle 1 \rangle$ (vale anche per -1), dato che $\forall k \in \mathbb{Z}$ è vero che $k = 1^k = 1 + 1 + 1 ... + 1$ k-volte.
Anche $(\mathbb{Z}_n, +)$ è ciclico, dato che $\mathbb{Z}_n = \langle [1] \rangle$.

8.4.2 Classi Laterali Destre e Sinistre

Introduciamo adesso quelle che sono le *classi laterali* di un sottogruppo.
Sia H un sottogruppo di $(G, *)$, dove G non è necessariamente finito, l'insieme H ha una **classe laterale sinistra** associata ad ogni $a \in G$, ed è l'insieme $aH = \{a * h, h \in H\}$, analogamente, la **classe laterale sinistra** associata ad ogni $a \in G$, è l'insieme $Ha = \{h * a, h \in H\}$, a meno che $(G, *)$ non sia commutativo, $aH \neq Ha$.
Esempio : consideriamo il gruppo simmetrico S_3, ed il suo sottogruppo $H = \left\{1, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\right\}$, prendo $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, avrò che :

$$aH = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} \qquad Ha = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

Seguono 3 importanti **proposizioni** :

- (1) $a, b \in G$, $aH = bH \iff a^{-1} * b \in H$
- (2) $a, b \in G \implies aH = bH$ oppure $aH \cap bH = \emptyset$
- (3) $\forall x \in G \exists a \in G | x \in aH$

Osservando le proposizioni (1),(2) e (3), risulta chiaro che, tutte le classi laterali sinistre forniscono una *partizione* di G, che denotiamo con $\mathcal{L}_S$.
Tale partizione $\mathcal{L}_S$, definisce anche una relazione di equivalenza :

$$a\rho_S b \iff \exists g \in G | a \in gH \wedge b \in gH$$

Osservazione : $a\rho_S b \iff a^{-1} * b \in H$.
Esiste la partizione analoga $\mathcal{L}_D$, con le classi laterali destre, che definisce la relazione :

$$a\rho_D b \iff a * b^{-1} \in H$$

In generale, $\rho_S \neq \rho_D$. Se G è finito, **l'indice** di H in G è il numero di classi laterali sinistre, che è uguale al numero di classi laterali destre.

8.4.3 Teorema di Lagrange

Sia $(G, *)$ un gruppo finito, e H un suo sottogruppo, vale che la cardinalità dell'insieme H *divide* la cardinalità dell'insieme G, l'ordine di H è un divisore dell'ordine di G.

$$|G| = i \cdot |H|$$

Dimostrazione : Sia H un sottogruppo di $(G, *)$ osserviamo che, esiste una mappa biettiva φ fra H ed una classe laterale sinistra $\varphi : H \to aH \ \forall a$, tale mappa è definita come :
$h \to a * h$, quindi, la cardinalità di H è uguale alla cardinalità di aH.
Consideriamo adesso $\{a_1H, a_2H, a_3H..., a_iH\}$, ossia l'insieme di tutte le classi laterali distinte.
Essendo che le classi definiscono una partizione, e sono fra loro tutte disgiunte, risulta chiaro che la somma delle loro cardinalità da la cardinalità di G :

$$|G| = \sum_{j=1}^{i} |a_j H| \tag{46}$$

Inoltre, è anche ovvio che le partizioni ricoprono totalmente G :

$$G = \bigcup_{j=1}^{i} (a_j H) \tag{47}$$

Le classi laterali hanno tutte la stessa cardinalità, quindi se sono in numero i, e vale che, per un qualsiasi a, la cardinalità di H è uguale alla cardinalità di aH, è vero che $|G| = i \cdot |H|$. ■

Proposizione : $\rho_S = \rho_D \iff aH = Ha \ \forall a \in G$

Definizione : Se $\rho_S = \rho_D$, allora H è detto sottogruppo **normale** e si denota con $H \trianglelefteq G$.

Proposizione : $H \trianglelefteq G \iff a * h * (a^{-1}) \in H \ \forall a \in G$.

8.4.4 Nucleo di un Omomorfismo

Se φ è un omomorfismo, l'insieme $Ker\varphi = \{g \in G | \varphi(g) = 1_G\}$ è detto **nucleo** di φ ed è un sotto-gruppo di G, è di facile dimostrazione :

$$\varphi(g_1 \cdot g_2^{-1}) = \varphi(g_1) \cdot \varphi(g_2^{-1}) = \varphi(g_1) \cdot \varphi(g_2)^{-1} = 1_G \cdot 1_G = 1_G \in Ker\varphi \tag{48}$$

Proposizione : φ è iniettiva $\iff Ker\varphi = \{1_G\}$.
Dimostrazione : Inizianmo dimostrando $\boxed{\varphi \text{ è iniettiva } \implies Ker\varphi = \{1_G\}}$, L'ipotesi è che φ sia iniettiva, predno un qualsiasi $g \in Ker\varphi$, ed ho che $\varphi(g) = 1_G = \varphi(1_G)$, ma dato che φ è iniettiva, ciò è vero se e solo se $g = 1_G$, quindi $Ker\varphi = \{1_G\}$. Adesso dimostriamo $\boxed{Ker\varphi = \{1_G\} \implies \varphi \text{ è iniettiva}}$, ho che $\varphi(g) = \varphi(g')$, ed inoltre $\varphi(g) \cdot \varphi(g')^{-1} = 1_G$, ed essendo che φ è un omomorfismo, ho $\varphi(g \cdot g'^{-1}) = 1_G$, per ipotesi
$g \cdot g'^{-1} \in Ker\varphi \implies g \cdot g'^{-1} = 1_G \implies$ moltiplico per $g' \implies g = g' \implies \varphi$ è iniettiva. ■

8.5 Struttura dei Gruppi Ciclici

Abbiamo già dato la definizione di gruppo ciclico, ossia un gruppo G, per cui risulta che, preso $g \in G$, si ha che $G = \langle g \rangle$.

8.5.1 Ordine di g

Definizione : In un gruppo ciclico G per cui $G = \langle g \rangle$, sia n il numero intero *più piccolo* maggiore di tale che $g^n = 1$, si dice che g ha **ordine** n e si denota $o(g) = n$, se tale n non esiste, allora g ha ordine infinito.

$$o(g) = \min(n \geq 1 | g^n = 1) \tag{49}$$

Proposizione : Se $G = \langle g \rangle$ e $o(g) = n$, allora $G = \{1, g, g^2, g^3 ..., g^{n-1}\}$.
È chiaro che, se un l'ordine del generatore è finito, allora il gruppo ha cardinalità finita.

Se un gruppo è ciclico, quindi $G = \langle g \rangle$, esso è generato o da un elemento di ordine finito, oppure da un elemento di ordine infinito, vediamo nel dettaglio i due casi :

Caso 1 $o(g) = \infty$: g è il generatore del gruppo G, definisco un applicazione $\varphi : \mathbb{Z} \to G$ definita come $\varphi : m \to g^m$, si ricordi che $\mathbb{Z} = \langle 1 \rangle$, tale applicazione, è un *omomorfismo* :

$$\varphi(m + n) = g^{m+n} \tag{50}$$

Risulta essere anche biettiva, è quindi un *isomorfismo*, essendo ovviamente iniettiva, $Ker\varphi = \{0\}$, ricordando com'è definito il nucleo :

$$Ker\varphi = \{m \in \mathbb{Z} | \varphi(m) = 1_G\} = \{m \in \mathbb{Z} | g^m = 1_G\}$$

Si noti che il più piccolo elemento di tale insieme è proprio $o(g)$, che però sappiamo per ipotesi essere infinito, quindi l'unico $m \in \mathbb{Z} | g^m = 1_G$ è esattamente $m = 0 \implies Ker\varphi = \{0\}$.
Osservazione : Se φ è un isomorfismo, allora stabilisce una corrispondenza biunivoca fra i sottogruppi di G.
Esiste un unico gruppo ciclico infinito (a meno di isomorfismi) ed è $(\mathbb{Z}, +)$.
Caso 2 $o(g) = n$: g è il generatore del gruppo G, definisco un applicazione $\varphi : \mathbb{Z}_{\ltimes} \to G$ definita come $\varphi : [m] \to g^m$, tale φ è ben definita ed è un omomorfismo :

$$\text{se } [m] \equiv [m'] \implies m' = m + nk \implies g^{m'} = g^{m+nk} = g^m * g^{nk} = g^m * (g^n)^k \tag{51}$$

Si ricordi che $g^n = 1_G$:

$$g^m * g^{nk} = g^m * 1_G^k = g^m \text{ abbiamo dimostrato che } [m] \equiv [m'] \implies g^m = g^{m'} \tag{52}$$

Inoltre essendo $G = \{1, g, g^2, g^3..., g^{n-1}\}$, ho che $\forall k \in \mathbb{Z}, k \to g^k$, φ è suriettiva. Essendo che $|G| = |\mathbb{Z}_n|$, φ è biettiva.

Fatta questa breve disquisizione possiamo enunciare un importante teorema, non prima però di una fondamentale *Osservazione* : Abbiamo visto che, $H \leq (\mathbb{Z}, +) \implies \exists n \in \mathbb{Z} | H = n\mathbb{Z}$, e che $H \leq (\mathbb{Z}_n, +) \implies H = H_d = \{[d], [2d]..., [(k-1)d, [0]]\}$ con $n = dk$. Si ricordi che un isomorfismo $\varphi : G \to G'$ definisce una corrispondenza biunivoca fra i sottogruppi di G e G'.

8.5.2 Teorema di Struttura dei Gruppi Ciclici

1. Se $H \leq G = \langle g \rangle$, allora H è ciclico.
2. Se $H \leq G = \langle g \rangle$ e $|G| = n = o(n)$, allora l'ordine di H divide n.
3. $\forall k | n = k \cdot c$ per qualche c (per ogni k divisore di n), $\exists! H \leq G | |H| = k \implies H = \left\langle g^{\frac{n}{k}} \right\rangle$

Se $G = \langle g \rangle$ e $o(g) = n$ allora esiste una corrispondenza biunivoca tra i divisori di n ed i sottogruppi di G.

$$\{\text{divisori di } n\} \to \text{ sottogruppi di } g$$
$$k \to \left\langle g^{\frac{n}{k}} \right\rangle$$

Notare che $|\left\langle g^{\frac{n}{k}} \right\rangle| = k$. Se $h|k \wedge k|n$, allora $\left\langle g^{\frac{n}{h}} \right\rangle$ è un sottogruppo di $\left\langle g^{\frac{n}{k}} \right\rangle$.

8.5.3 Proprietà dell'Ordine

Proposizione : In un gruppo $(G, \cdot)$ se $g^t = 1$ (assumendo che $o(g) < \infty$), allora $o(g)$ divide t. Ciò è di facile dimostrazione, se $o(g)$ divide t si ha $t = k \cdot o(n) + r$ con $r < o(g)$, si ha che $g^t = g^{ko(g)+r} = (g^{o(g)})^k \cdot g^r = 1 \iff r = 0$. ■

Vediamo una **proprietà aritmetica** dell'ordine, se $o(g) < \infty$, allora :

$$o(g^s) = \frac{\text{mcm}(o(g), s)}{s} = d$$

Preso un omomorfismo $\varphi : G \to G'$, è lecito chiedersi se in qualche modo c'è un collegamento fra $o(g)$ e $o(\varphi(g))$. Si vedano le seguenti proposizioni :
Proposizione 1 : $o(\varphi(g))$ divide $o(g)$.
Dimostrazione 1 : $1 = g^{o(g)} \implies \varphi(1) = \varphi(g^{o(g)})$, essendo che φ è un omomorfismo, riscrivo quest'ultimo come $\varphi(g)^{o(g)}$, si ricordi che per qualsiasi omomorfismo, $\varphi(1) = 1$, quindi $\varphi(g^{o(g)}) = \varphi(g)^{o(g)} = 1$, per la definizione di ordine, per la definizione di ordine appena vista, $o(\varphi(g))|o(g)$. ■
Proposizione 2 : Se φ è iniettiva, allora $o(\varphi(g)) = o(g)$.

Dimostrazione 2 : $G = \{1, g..., g^{o(g)-1}\}$ presenta elementi a coppie distinti, essendo φ iniettiva, anche le loro immagini risultano a coppie distinte, per definizione di ordine, $o(\varphi(g)) \geq o(g)$, necessariamente $o(\varphi(g)) = o(g)$. ■ Attenzione ! Questa specifica dimostrazione, l'ho copiata per come l'ho scritta dagli appunti presi in classe, non mi è chiara e credo di essermi perso qualcosa, chiunque disponga di una dimostrazione completa, è pregato di scrivermi in modo tale che io possa aggiornare e correggere questa sezione.

Teorema : Sia n primo, allora $(\mathcal{U}(\mathbb{Z}_n), \cdot) \simeq (\mathbb{Z}_{n-1}, +)$, esiste un $a \in \mathcal{U}(\mathbb{Z}_n)$ per cui $o(a) = n - 1$.
Per dimostrare tale teorema si necessita di alcune osservazioni e proposizioni :

Proposizione : Sia G un gruppo commutativo, se $a, b \in G$ di ordine $o(a) = n$ e $o(b) = m$, allora esiste $c \in G$ tale che $o(c) = \text{mcm}(o(a), o(b))$.
Dimostrazione della proposizione : Consideriamo l'elemendo ab e calcoliamone l'ordine, osserviamo che $(ab)^{mn} = (a^n)^m \cdot (b^m)^n = 1 \implies o(ab)$ divide mn, tuttavia, non è detto che $o(ab) = mn$, infatti, si prenda il caso $a = x$ e $b = x^{-1}$, si ha che $ab = 1$, e
$1 = o(1) < o(a) = o(b) = n$.
In generale, se $(ab)^t = 1$, allora $1 = (ab)^t = a^t b^t \implies a^t = b^{-t} \implies o(a) = o(b^{-t})$. Ciò suggerisce la seguente osservazione.

Osservazione 1 : Se $n = o(a)$ e $m = o(b)$ sono coprimi, allora $o(ab) = nm = mcm(n, m)$.
Dimostrazione dell'osservazione 1 : Per quanto visto sopra,
$a^{o(ab)} = b^{-o(ab)} \implies 1 = (a^{o(ab)})^n = (b^{-o(ab)})^n = b^{-n \cdot o(ab)} \implies o(b) = m$ divide $n \cdot o(ab)$,
essendo m ed n coprimi, necessariamente m divide $o(ab)$, analogamente, si ha l'identità
$1 = a^{m \cdot o(ab)}$, ed implica che n divide $o(ab)$, di conseguenza, nm divide $o(ab)$, che è ciò che si voleva dimostrare nell'osservazione 1. $\square$
Tornando alla proposizione, rimane da considerare il caso in cui n, m abbiano fattori comuni, ciò si riduce al caso precedente nel seguente modo :
Si fattorizza in primi :

$$\text{mcm}(n, m) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} ... \cdot p_k^{\alpha_k} \tag{53}$$

Ogni fattore $p_i^{\alpha_i}$ o divide n oppure divide m (si è visto nel capitolo 2.5.1), se G contiene un elemento g di ordine s, e d divide s, allora G contiene un elemento di ordine d, questo ci permette di costruire per ogni $j = 1, 2..., k$ un elemento c_j per cui $o(c_j) = p_j^{\alpha_j}$. Consideriamo il prodotto di tutti questi elementi : $c := c_1 \cdot c_2..., \cdot c_k$, si noti :

Osservazione 2 : $o(c) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} ... \cdot p_k^{\alpha_k} = \text{mcm}(n, m)$.
Dimostrazione dell'osservazione 2 : Facciamo induzione sul parametro k, ossia il numero di fattori :
caso base : $o(c_1 \cdot c_2..., \cdot c_j) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} ... \cdot p_j^{\alpha_j}$
ipotesi induttiva : $o(c_1 \cdot c_2..., \cdot c_{j+1}) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} ... \cdot p_{j+1}^{\alpha_{j+1}}$
Siccome $o(c_1 \cdot c_2..., \cdot c_j)$ e $o(c_{j+1})$ sono coprimi, posso applicare l'*osservazione 1* e trovare che $o((c_1 \cdot c_2..., \cdot c_j) \cdot o(c_{j+1})) = o(c_1 \cdot c_2..., \cdot c_j) \cdot o(c_{j+1})$ come volevasi dimostrare, quindi abbiamo dimostrato l'osservazione 2 e la proposizione. $\square$
Applichiamo adesso la proposizione per dimostrare il teorema.

Dimostrazione del teorema : Vogliamo vedere che $\exists a \in \mathcal{U}(\mathbb{Z}_n) | o(a) = n - 1$. Possiamo prendere un elemento di ordine massimo, dato che $\mathcal{U}(\mathbb{Z}_n)$ è finito, ogni elemento ha ordine finito, prendiamo allora $a \in \mathcal{U}$ tale che $o(a) = m$, dove m è l'ordine massimo :
$\forall h \in G, o(h) \leq m = o(a)$. Chiaramente, $m \leq n - 1$, ma a priori non vale l'uguaglianza, notiamo la seguente osservazione :

Osservazione 3 : Ogni elemento $b \in \mathcal{U}(\mathbb{Z}_n)$ ha ordine che divide l'ordine massimo $m = o(a)$.
Dimostrazione dell'osservazione 3 : Si utilizza la *proposizione*, se esistesse b di ordine che non divide $m = o(a)$, allora, essendo $\mathcal{U}(\mathbb{Z}_n)$ commutativo, esisterebbe $c \in \mathcal{U}(\mathbb{Z}_n)$ di ordine $o(c) = \text{mcm}(o(a), o(b)) > o(a)$ (dato che $o(b)$ non divide $o(a)$). Tuttavia, era stato scelto a che

ha ordine massimo, questo produce una contraddizione e dimostra l'osservazione 3. □. Dunque, $\forall b \in \mathcal{U}(\mathbb{Z}_n), b^m = 1$ dove $m = o(a)$, in altri termini, $b \in \mathcal{U}(\mathbb{Z}_n)$ non è altro che una soluzione del polinomio $x^m - 1 = 0$ a coefficenti nel campo $\mathbb{Z}_n$ (si è usato il termine campo perché n è primo, come si è visto nel capitolo 4.2.1), essendo un campo, per il teorema fondamentale dell'algebra 6.2, il polinomio $x^m - 1 = 0$ ha al più m soluzioni. Ne deduciamo che $m \geq |\mathcal{U}(\mathbb{Z}_n)| = n - 1$, e di conseguenza, che $m = n - 1$. ■