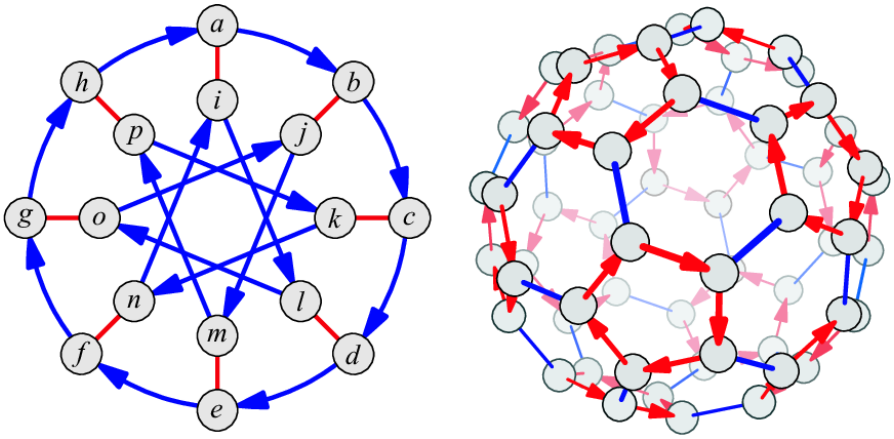
APPUNTI DI ALGEBRA

Manuel Deodato



Indice

1 Gli interi

1.1 Proprietà di base

Una proprietà dei numeri interi, che si prenderà come assiomatica, è quella del *buon ordinamento*:

Ogni insieme non-vuoto di interi maggiori o uguali a 0, *ha un elemento minimo.*

Da questa deriva la seguente.

Teorema 1.1 (Principio di induzione (prima forma))
Sia $A(n)$ un'affermazione valida per ogni intero $n \geq 1$. Se

(1). $A(1)$ è vera,

(2). $\forall n \geq 1$, se $A(n)$ è vera $\implies A(n+1)$ è vera,

allora, $\forall n \geq 1$, $A(n)$ è vera.

Dimostrazione. Sia S l'insieme di interi per cui $A(n)$ è falsa. Si mostra che S è l'insieme vuoto. Si assume per assurdo che $S \neq \varnothing \Rightarrow \exists n_0 \in S$, con n_0 minimo (esistente per il buon ordinamento), e, per assunzione, deve essere $n_0 \neq 1 \Rightarrow n_0 > 1$. Questo vuol dire che $n_0 - 1$ non è in S e, quindi, $A(n_0 - 1)$ è vera.
Per la proprietà (2), però, deve essere vera anche $A(n_0)$ perché $n_0 = (n_0 - 1) + 1$, il che è assurdo e, pertanto, $S = \varnothing$. □

Osservazione 1.1. Nella dimostrazione sopra, si sarebbe potuto sostituire 1 con 0 e far partire il principio di induzione da $n = 0$ piuttosto che da $n = 1$ e non sarebbe cambiato nulla.

Il principio di induzione può essere espresso in una forma alternativa, come segue.

Teorema 1.2 (Principio di induzione (seconda forma))
Sia $A(n)$ affermazione vera $\forall n \geq 0$ e sia possibile mostrare che:

(1'). $A(0)$ è vera;

(2'). $\forall n > 0$, se $A(k)$ è vera $\forall 0 \leq k < n$, allora $A(n)$ è vera.

Allora $A(n)$ è vera $\forall n \geq 0$.

Dimostrazione. Sia ancora S l'insieme degli interi che non soddisfano $A(n)$. Ancora per assurdo, si prende $S \neq \varnothing$, quindi deve esistere, per il buon ordinamento, un $n_0 \in S$ minimo.
Per punto (1'), deve valere $n_0 \neq 0$ e, visto che n_0 è minimo, $\forall k$ intero tale che $0 \leq k < n_0$, $A(k)$ deve essere vera. Per il punto (2'), però, deve essere vera anche $A(n_0)$, arrivando nuovamente all'assurdo. □

Un altro importante risultato del buon ordinamento è l'*algoritmo di Euclide*.

Teorema 1.3 (Algoritmo di Euclide)

Siano m, n interi, con $m > 0$; allora esistono interi q, r, con $0 \leq r < m$, tali che

$$n = qm + r \tag{1.1.1}$$

Inoltre, gli interi q, r sono univocamente determinati da tali condizioni.

Dimostrazione. Visto che l'insieme degli interi q tali per cui $qm \leq n$ è limitato superiormente per definizione, si può usare il buon ordinamento per affermare che esiste un elemento più grande[a] tale che

$$qm \leq n < (q+1)m = qm + m$$

ossia $0 \leq n - qm < m$. Sia $r = n - qm$, per cui vale $0 \leq r < m$. Questo dimostra l'esistenza di r, q come descritti.
Per l'unicità, si assume che valga contemporaneamente

$$\begin{cases} n = q_1 m + r_1 & , \ 0 \leq r_1 < m \\ n = q_2 m + r_2 & , \ 0 \leq r_2 < m \end{cases}$$

con $r_1 \neq r_2$. Sia, per esempio, $r_2 > r_1$; allora, sottraendo le due, si ha $(q_1 - q_2)m = r_2 - r_1$. Però, si ha $r_2 - r_1 > 0$ e $r_2 - r_1 < m$, il che non è possibile perché $q_1 - q_2$ è un intero per cui $(q_1 - q_2)m > 0$, quindi si avrebbe $r_2 - r_1 = (q_1 - q_2)m \geq m$ e, quindi $r_2 - r_1 \geq m$. Pertanto, deve essere $r_1 = r_2$, che fra l'altro implica $q_1 m = q_2 m$, per cui $q_1 = q_2$. □

[a] Basta applicare il buon ordinamento all'elemento più piccolo dell'insieme $n - qm$.

Da questo teorema, si definisce r come il *resto della divisione di n per m*.

1.2 Massimo comune divisore

Siano n, d due interi diversi da 0. Si dice che d *divide* n se esiste q intero tale che $n = dq$; in questo caso, si scrive $d|n$. Se m, n sono interi non-nulli, per *divisore comune* di m e n si intende un intero $d \neq 0$ tale che $d|m$ e $d|n$. Allora si ha la seguente definizione.

Definizione 1.1 (Massimo comune divisore)

Per massimo comune divisore di m, n interi non nulli, si intende un intero $d > 0$, divisore comune di m e n, e tale che $\forall e$ intero positivo che divide m e n, si ha anche $e|d$.

Chiaramente, il massimo comune divisore è univocamente determinato e si mostrerà che esiste sempre. Per farlo, si dà prima la seguente definizione.

Definizione 1.2 (Ideale)

Sia $J \subseteq \mathbb{Z}$ un sottoinsieme degli interi. Si dice che J è un *ideale* se:

- $0 \in J$;
- $m, n \in J \implies m + n \in J$
- se $m \in J$ e n è un intero qualsiasi, allora $mn \in J$.

Osservazione 1.2. Di seguito, per ideale si intenderà sempre un sottoinsieme degli interi.

Siano $m_1, \ldots, m_r$ interi. Sia J l'insieme di tutti gli interi che si scrivono come

$$x_1 m_1 + \ldots + x_r m_r$$

con $x_1, \ldots, x_r$ interi. Allora è automaticamente verificato che J è un ideale. Infatti

- se $y_1, \ldots, y_r$ sono interi, allora

  $$\sum_{i=1}^{r} x_i m_i + \sum_{j=1}^{r} y_j m_j = (x_1 + y_1)m_1 + \ldots + (x_r + y_r)m_r$$

  che, quindi, appartiene a J;

- se n è un intero, si ha

  $$n \sum_{i=1}^{r} x_i m_i = n x_1 m_1 + \ldots + n x_r m_r$$

  che, quindi, appartiene a J;

- si può scrivere 0 come $0m_1 + \ldots + 0m_r$, quindi anche $0 \in J$.

In questo caso, si dice che J è **generato** dagli interi $m_1, \ldots, m_r$ e che questi sono i suoi **generatori**. L'insieme $\{0\}$ è esso stesso un ideale, chiamato **ideale nullo**. Inoltre, $\mathbb{Z}$ è detto **ideale unità**. Ora si può dimostrare il seguente.

Teorema 1.4

Sia J un ideale di $\mathbb{Z}$. Allora esiste un intero d che è un generatore di J. Inoltre, se $J \neq \{0\}$, allora d è il più piccolo intero positivo in J.

Dimostrazione. Sia J l'ideale nullo; allora 0 è un suo generatore. Sia, ora, $J \neq \{0\}$; se $n \in J$, allora $-n = (-1)n$ è anche in J, quindi J contiene degli interi positivi. Si vuole dimostrare che d, definito come il più piccolo intero positivo, è un generatore. Per farlo, sia $n \in J$, con $n = dq + r$, $0 \leq r < d$; allora $r = n - dq \in J$ e, visto che vale $r < d$, segue che $r = 0$[a], quindi $n = dq$ e, allora, d è un generatore. □

[a] Altrimenti d non sarebbe il più piccolo intero positivo.

Teorema 1.5

Siano m_1, m_2 due interi positivi e sia d un generatore positivo per l'ideale generato da m_1, m_2. Allora d è il massimo comune divisore di m_1, m_2.

Dimostrazione. Per definizione, $m_1, m_2 \in J$[a], quindi esiste un intero q_1 tale che $m_1 = q_1 d$, per cui $d|m_1$. Analogamente $d|m_2$. Sia, poi, e un intero non-nullo che divide sia m_1 che m_2 come $m_1 = h_1 e$ e $mm_2 = h_2 e$, con interi h_1, h_2. Visto che d è nell'ideale generato da m_1, m_2, esistono degli interi s_1, s_2 tali che $d = s_1 m_1 + s_2 m_2$, quindi

$$d = s_1 h_1 e + s_2 h_2 e = (s_1 h_1 + s_2 h_2) e$$

Quindi e divide d e il teorema è dimostrato. □

[a] Questo è ovvio perché $m_1 = 1m_1 + 0m_2$ e $m_2 = 0m_1 + 1m_2$.

Osservazione 1.3. La stessa esatta dimostrazione funziona per più di due interi, quindi se si considerassero $m_1, \ldots, m_r$ degli interi, con d generatore positivo dell'ideale da loro generato, d sarebbe anche il massimo comune divisore.

Questi due teoremi permettono di concludere i seguenti fatti.

- Ogni ideale J contiene un numero intero che lo genera interamente e questo coincide col più piccolo intero positivo in esso contenuto, quindi è l'unico generatore *singolo* dell'ideale.
- Ogni insieme di numeri interi ha un massimo comune divisore perché tale insieme genera un ideale, il quale, però, contiene un generatore (più piccolo numero intero in esso contenuto) che è un massimo comune divisore per l'insieme di interi iniziale.

Definizione 1.3 (Interi coprimi)

Siano $m_1, \ldots, m_r$ degli interi il cui massimo comune divisore è 1. Allora $m_1, \ldots, m_r$ si dicono *coprimi* e, per questi, esistono interi $x_1, \ldots, x_r$ tali che

$$x_1 m_1 + \ldots + x_r m_r = 1$$

perché 1 appartiene all'ideale generato dagli m_i.

È immediato verificare per definizione di ideale che $1 \in J \iff J \equiv \mathbb{Z}$. Dalla definizione 1.3 segue direttamente che ogni insieme di interi coprimi genera $\mathbb{Z}$.

Osservazione 1.4. Si potrebbe pensare che se p è un numero primo, allora l'insieme $\{p\}$ generi $\mathbb{Z}$, cioè p generi $\mathbb{Z}$. Questo è ovviamente falso sia perché, evidentemente, J_p non contiene 1, sia perché p non è coprimo con se stesso, avendo come altro divisore proprio p oltre che 1.

1.3 Fattorizzazione unica

Definizione 1.4 (Numero primo)
Si dice che p è un numero primo se è un intero e $p \geq 2$ tale che, data una fattorizzazione $p = mn$, con interi positivi m, n, allora $m = 1$ o $n = 1$.

Osservazione 1.5. Il fatto che $p = mn$ con $m = 1$, o $n = 1$ implica p numero primo significa che p è diviso unicamente o da 1 o, da se stesso.

Ora si mostra che ogni numero intero ammette un'unica scomposizione in numeri primi. Per dimostrare l'unicità di tale scomposizione, si introduce il seguente lemma.

Lemma 1.1
Sia p un numero primo e siano m, n interi non-nulli e tali che p divide mn. Allora o $p|m$ o $p|n$.

Dimostrazione. Senza perdita di generalità, si assume che p *non* divida m. Allora, il massimo comune divisore di p e m deve essere 1, pertanto esistono interi a, b tali per cui $1 = ap + bm$.
Ora, moltiplicando ambo i membri per n, si ha $n = nap + bmn$, ma $mn = pc$ per qualche intero c (essendo in assunzione mn divisibile per p), quindi

$$n = nap + bpc = (na + bc)p$$

il che implica che p divide n. □

Per evidenziare l'utilità del lemma nel seguente teorema, si nota che se p divide un prodotto di numeri primi $q_1 \dots q_s$, si hanno due possibilità: o p divide q_1, o divide $q_2 \dots q_s$; se divide q_1, allora $p \equiv q_1$, altrimenti si trova $p \equiv q_i$ procedendo induttivamente. Il caso interessante è quando si ha un uguaglianza tra prodotti di numeri primi

$$p_1 \dots p_r = q_1 \dots q_s$$

dove ogni p_i divide il prodotto[1]. Rinumerandoli, si può assumere senza perdita di generalità che $p_1 = q_1$ e, induttivamente, che $p_i = q_i$ e $r = s$, essendo due scomposizioni in un numeri primi.

Teorema 1.6
Ogni intero positivo $n \geq 2$ ammette una fattorizzazione come prodotto di numeri primi (non necessariamente distinti) $n = p_1 \dots p_r$ e tale fattorizzazione è unica.

Dimostrazione. Si assume per assurdo che esista almeno un intero ≥ 2 che non possa essere espresso come prodotto di numeri primi. Sia m il più piccolo di

[1] Per vederlo, è sufficiente prendere $c = p_1 \dots p_{i-1} p_{i+1} \dots p_r$, quindi si ha $cp_i = q_1 \dots q_s$, che è la definizione di $p_i | q_1 \dots q_s$.

questi.
Per costruzione, m non può essere primo, quindi $m = de$, con $d, e > 1$. Visto che d ed e sono minori di m e visto che m è scelto per essere il più piccolo fra gli interi non fattorizzabili come numeri primi, allora sia d che e ammettono scomposizione in prodotto di numeri primi:

$$\begin{aligned} d &= p_1 \dots p_r \\ e &= p'_1 \dots p'_s \end{aligned} \implies m = p_1 \dots p_r p'_1 \dots p'_s$$

da cui l'assurdo.
Per mostrare l'unicità, si usa il lemma 1.1. Come conseguenza, diretta del lemma, se esistessero due scomposizioni in primi $p_1 \dots p_r$ e $p'_1 \dots p'_s$, varrebbe $p_1 \dots p_r = p'_1 \dots p'_s \Rightarrow p_i = p'_i$ e $r = s$, da cui l'unicità □

1.4 Identità di Bézout e equazioni diofantee

1.4.1 Identità di Bézout

L'identità di Bézout non è altro che quanto espresso in teorema 1.5. Di seguito lo si enuncia senza ricorrere a tale trattazione.

Teorema 1.7 (Identità di Bézout)
Dati $a, b \in \mathbb{Z}$ non entrambi nulli, esistono altri due interi m, n tali che:

$$\gcd(a, b) = am + bn$$

Dimostrazione. Si considera l'insieme di tutte le possibili combinazioni lineari positive di a, b, dato da $\mathrm{CL}^+(a, b) := \{ar + bs : r, s \in \mathbb{Z},\ ar + bs > 0\}$. Questo è non-vuoto perché, assumendo senza perdita di generalità $a \neq 0$, esistono, per $s = 0$, degli $r \in \mathbb{Z}$ tali che $ra > 0$.
Visto che $\mathrm{CL}^+(a, b) \subseteq \mathbb{N}$, per il principio del buon ordinamento, questo ammette un minimo d; in quanto tale $\exists m, n \in \mathbb{Z} : d = am + bn$. Infine, si motra che $d = \gcd(a, b)$, cioè si mostrano i seguenti punti.

- Si ha $d|a$ e $d|b$.

  Dividendo a per d, si ha $a = qd + r$, con $0 \leq r < d$, quindi

  $$a = q(am + bn) + r$$

  da cui

  $$r = (-qm + 1)a + (-qn)b$$

  In questo modo, r è combinazione lineare di a, b ed è minore di d, ma questo

è assurdo perché d era minimo per assunzione, quindi deve essere $r = 0$. Allo stesso modo si mostra $d|b$.

- Se $c|a$ e $c|b \implies c \leq d$.

  Questo è vero perché se $c|a,\ c|b$, allora (in particolare) $c|(am+bn)$, cioè $c|d \Rightarrow c \leq d$.

□

Osservazione 1.6. Il teorema afferma l'esistenza di una possibile coppia $(m,n) \in \mathbb{Z}\times\mathbb{Z}$ che soddisfa $\gcd(a,b) = am+bn$, ma non ne specifica l'unicità; di fatto, si vedrà che di coppie simili ce ne sono infinite.

Corollario 1.1

Dati $a,b \in \mathbb{Z}$ non entrambi nulli e sia $c \in \mathbb{Z} : c|a$ e $c|b$; allora $c|\gcd(a,b)$.

Complessivamente, esattamente come riportato nel teorema 1.5, si è dimostrato che il massimo comune divisore di due interi a,b è la più piccola combinazione lineare positiva ottenibile dai due.

Corollario 1.2

Dati a,b non entrambi nulli e $\gcd(a,b)$ il loro massimo comune divsore, allora gli interi

$$a' = \frac{a}{\gcd(a,b)} \qquad\qquad b' = \frac{b}{\gcd(a,b)}$$

sono coprimi.

Dimostrazione. Si può dimostrare in due modi diversi. Nel primo, si assume per assurdo che esista un divisore comune $d > 1$ di a', b'; se così fosse, però, $d \cdot \gcd(a,b)$ dividerebbe sia a che b e sarebbe più grande di $\gcd(a,b)$ stesso, il che è assurdo.
Il secondo fa uso dell'identità di Bézout per cui $\gcd(a,b) = am + bn$; dividendo per $\gcd(a,b)$, si ha:

$$1 = a'm + b'n$$

per cui 1 è il più piccolo intero positivo ottenibile come combinazione lineare positiva di a', b', quindi i due sono coprimi. □

Teorema 1.8

Siano $a,b,c \in \mathbb{Z}$; se $a|bc$ e $\gcd(a,b) = 1$, allora $a|c$.

Dimostrazione. Per Bézout, visto che $\gcd(a,b) = 1$, si ha $1 = an+bm$ per una coppia di numeri $m,n \in \mathbb{Z}$. Moltiplicando ambo i membri per c, ne segue che:

$$c = acn + bcm$$

quindi $a|c$ perché, ovviamente, $a|acn$, mentre $a|bcm$ perché, per ipotesi, $a|bc$,

quindi $a|(acn + bcm)$, cioè $a|c$. □

Il teorema appena dimostrato è alla base del fatto che la fattorizzazione di interi in numeri primi è unica.

1.4.2 Equazioni diofantee

Dati $a, b, c \in \mathbb{Z}$, si dice **equazione diofantea** un'equazione del tipo

$$ax + by = c \tag{1.4.1}$$

La sua soluzione è una coppia di interi $(\overline{x}, \overline{y}) \in \mathbb{Z} \times \mathbb{Z}$ che la soddisfa.

> **Osservazione 1.7.** L'equazione diofantea con $a = b = 0$ ha soluzione $\iff c = 0$ e ne ammette infinite, consistenti in tutte le possibili coppie $(\overline{x}, \overline{y}) \in \mathbb{Z} \times \mathbb{Z}$, perché ogni coppia soddisfa $0x + 0y = c$.

Per il caso generale di a, b non entrambi nulli, si ha il seguente.

Teorema 1.9

L'equazione $ax + by = c$, con a, b non entrambi nulli, ha soluzione $\iff \gcd(a, b)|c$.

Dimostrazione. Per l'identità di Bézout, si sa che vi è soluzione all'equazione

$$ax + by = \gcd(a, b)$$

L'equazione da risolvere è diversa: al posto di $\gcd(a, b)$ c'è c; allora la dimostrazione si basa sul capire se $\gcd(a, b)$ divide o meno c.
Nel caso in cui $\gcd(a, b)|c$ (per cui si ha $c = k \cdot \gcd(a, b)$ per qualche intero k), allora l'equazione diofantea ammette soluzione. Infatti, dopo aver trovato $(m, n) \in \mathbb{Z} \times \mathbb{Z}$ che risolve $am + bn = \gcd(a, b)$, si ha che $(mk, nk) \in \mathbb{Z} \times \mathbb{Z}$ risolve l'equazione diofantea perché

$$k \cdot (am + bn) = akm + bkn = k \cdot \gcd(a, b) = c$$

Viceversa, se $\gcd(a, b)$ non divide c, allora non vi è soluzione. Se, per assurdo, vi fosse soluzione, sia questa $(\overline{x}, \overline{y})$, allora $a\overline{x} + b\overline{y} = c$ implica che $\gcd(a, b)|c$ perché $\gcd(a, b)$ divide il membro di sinistra (essendo un divisore sia di a che di b). Questo, però, è assurdo perché si era nell'ipotesi in cui $\gcd(a, b) \nmid c$. □

Si considera il caso in cui l'equazione $ax + by = c$ ha soluzione; si vuole capire se la soluzione è unica, o se ve ne sono di più. Si considera, a tal proposito, l'**omogenea associata** $ax + by = 0$.

Osservazione 1.8. La comodità nel lavorare con l'omogenea associata sta nel fatto che se $(\overline{x}, \overline{y})$ risolve $ax + by = c$ e (γ, δ) risolve l'omogenea, allora $(\overline{x} + \gamma, \overline{y} + \delta)$ è ancora soluzione di $ax + by = c$.

L'obiettivo, ora, è di trovare il numero delle soluzioni per l'omogenea associata. Si nota che $ax + by = 0 \Rightarrow axa = -by$; si risolve

$$\frac{a}{\gcd(a,b)}x = -\frac{b}{\gcd(a,b)}y$$

Sia (γ, δ) una soluzione di questa; visto che $a/\gcd(a,b)$ e $b/\gcd(a,b)$ sono coprimi[1], il teorema 1.8 afferma che $a/\gcd(a,b)$ divide δ, quindi δ è della forma $\frac{a}{\gcd(a,b)}t$ e γ, analogamente, è della forma $-\frac{b}{\gcd(a,b)}t$.

Al contrario, si nota facilmente che una qualunque coppia della forma $\left(-\frac{b}{\gcd(a,b)}t, \frac{a}{\gcd(a,b)}t\right)$, con $t \in \mathbb{Z}$ è una soluzione dell'omogenea associata. Questo significa che le soluzioni dell'omogenea associata sono tutte di questa forma, pertanto sono infinite.

Da questo discorso, si può concludere che anche le soluzioni dell'equazione diofantea iniziale $ax + by = c$ sono infinite. Il teorema di seguito permette di concludere, ulteriormente, che *tutte* le soluzioni di $ax + by = c$ sono esprimibili tramite quelle dell'omogenea, quindi equazione originale e omogenea hanno lo stesso numero di soluzioni.

Teorema 1.10

Se l'equazione $ax + by = c$ ammette soluzione, allora ne ammette infinite. Data $(\overline{x}, \overline{y})$ una sua soluzione, l'insieme $\mathcal{S}$ di tutte le soluzioni di $ax + by = c$ è ottenibile come

$$\mathcal{S} = \{(\overline{x} + \gamma, \overline{y} + \delta) : (\gamma, \delta) \text{ soluzione dell'omogenea associata}\}$$

Dimostrazione. Per quanto detto sopra, si conclude che

$$\{(\overline{x} + \gamma, \overline{y} + \delta) : (\gamma, \delta) \text{ soluzione dell'omogenea associata}\} \subseteq \mathcal{S}$$

Si deve mostrare l'inclusione inversa. Questo segue direttamente dal fatto che, se (α, β) è soluzione di $ax + by = c$, allora $(\alpha - \overline{x}, \beta - \overline{y})$ è soluzione dell'omogenea associata. □

1.5 Relazioni di equivalenza e congruenza

Definizione 1.5 (Relazione di equivalenza)

Sia S un insieme. Una relazione di equivalenza su S è una relazione indicata con $x \sim y$, $x, y \in S$, tale che:

ER 1. $\forall x \in S,\ x \sim x$;

[1] Vedi corollario 1.2.

ER 2. se $x \sim y$ e $y \sim z$, allora $x \sim z$;

ER 3. se $x \sim y$, allora $y \sim x$.

Se su S è definita una relazione di equivalenza $\sim$, le classi di equivalenza sono insiemi $C_x := \{y \in S : y \sim x\}$ partizionano S in insiemi disgiunti. Inoltre, dati due elementi $r, s \in S$, si ha $C_r \equiv C_s$, oppure C_r, C_s non hanno elementi in comune. Si sceglie un elemento che identifica la classe di equivalenza, ad esempio x per C_x, e tale elemento si chiama rappresentante della classe di equivalenza. Un esempio di relazione di equivalenza è la congruenza.

Definizione 1.6 (Congruenza)

Sia $m \in \mathbb{Z}^+$ e $a, b \in \mathbb{Z}$; si dice che a è *congruente b modulo m* se $\exists k \in \mathbb{Z} : a - b = km$. In tal caso, si scriverà $a \equiv b \pmod{m}$.

Osservazione 1.9. La definizione più esplicativa di congruenza è che due numeri $a, b \in \mathbb{Z}$ di dicono congruenti modulo $m \in \mathbb{Z}^+$ se, divisi per m, restituiscono lo stesso resto. Di fatto, da questa discende la definizione data sopra: se $a = qm + r$, $b = pm + r \Rightarrow a - b = (q - p)m$.

Definizione 1.7 (Interi pari e dispari)

Si definiscono gli interi **pari** come quelli che sono congruenti a $0 \pmod{2}$ (quindi $n = 2m$) e quelli **dispari** come gli interi che non sono pari, quindi della forma $2m + 1$, per qualche intero m.

Dalla definizione di congruenza, si ha che $a \equiv b \pmod{m} \Rightarrow a - b = qm$, quindi $a - b$ appartiene all'ideale generato da m.

Inoltre, la stessa relazione implica che $m|(a - b)$; viceversa, se $a \not\equiv b \pmod{m}$, allora i due numeri divisi per m avrebbero resti diversi: $a = k_1 m + r_a$, $b = k_2 m + r_b$, il che implica che $a - b = (k_1 - k_2)m + (r_a - r_b)$, che non è divisibile per m; allora is ha il seguente.

Proposizione 1.1

Siano $m \in \mathbb{Z}^+$ e $a, b \in \mathbb{Z}$; a e b sono congruenti se e soltanto se $m|(a - b)$.

Proposizione 1.2 (Addizione e moltiplicazione in congruenza)

Dati $a \equiv a' \pmod{m}$ e $b \equiv b' \pmod{m}$, si ha:

$$a + b \equiv a' + b' \pmod{m}$$
$$ab \equiv a'b' \pmod{m}$$

Dimostrazione. Per definizione, si ha $a' = a + km$ e $b' = b + k'm$; quindi:

$$a' + b' = a + b + (k + k')m \implies a' + b' \equiv a + b \pmod{m}$$

Per la moltiplicazione, si nota che

$$a'b' = ab + m(kb + k'a) + kk'm^2$$

da cui si vede che $a'b' - ab$ è divisibile per m, quindi $a'b' \equiv ab \pmod{m}$. □

La divisione in congruenza funziona diversamente; infatti $2 \cdot 7 \equiv 2 \cdot 4 \pmod{6}$, ma $7 \not\equiv 4 \pmod{6}$. Si ha il seguente.

Teorema 1.11 (Divisione in congruenza)

Sia $m \in \mathbb{Z}^+$; $\forall a \in \mathbb{Z} \setminus \{0\}$ e dati $b_1, b_2 \in \mathbb{Z}$, vale

$$ab_1 \equiv ab_2 \pmod{m} \iff b_1 \equiv b_2 \mod \frac{m}{\gcd(a,m)}$$

Questo vuol dire che la divisione è ammessa a patto di dividere il modulo per $\gcd(a,m)$.

Dimostrazione. Si mostra l'implicazione verso destra. Per definizione, $m \mid (ab_1 - ab_2)$, quindi $\exists q \in \mathbb{Z} : mq = ab_1 - ab_2$. Dividendo per $\gcd(a,m)$:

$$\frac{a}{\gcd(a,m)}(b_1 - b_2) = \frac{m}{\gcd(a,m)}q$$

Ma $a/\gcd(a,m)$ e $m/\gcd(a,m)$ sono coprimi, quindi $\left(m/\gcd(a,m)\right) \mid (b_1 - b_2)$, il che implica che

$$b_1 \equiv b_2 \mod \frac{m}{\gcd(a,m)}$$

Per l'implicazione inversa, si assume che

$$b_1 \equiv b_2 \mod \frac{m}{\gcd(a,m)}$$

per cui $\exists t \in \mathbb{Z}$ tale che

$$t\frac{m}{\gcd(a,m)} = b_1 - b_2 \implies tm = (b_1 - b_2)\gcd(a,m)$$

quindi $m \mid (b_1 - b_2)\gcd(a,m)$. Usando che $\gcd(a,m) \mid a$, si ottiene che

$$m \mid (b_1 - b_2)a \implies ab_1 \equiv ab_2 \pmod{m}$$

□

1.5.1 Inversi in congruenze

Gli unici inversi moltiplicativi in $\mathbb{Z}$ sono $+1, -1$; operando con le congruenze, si riescono a trovare altri inversi moltiplicativi a patto di definire correttamente cosa vuol

dire.

Definizione 1.8 (Inverso in congruenza)

Sia $m \in \mathbb{Z}^+$; l'inverso di $a \in \mathbb{Z}$ è un certo $e \in \mathbb{Z}$ tale che

$$e \cdot a \equiv 1 \pmod{m}$$

Esempio 1.1. Per esempio, 2 è l'inverso di $3 \bmod 5$ perché $2 \cdot 3 = 6 \equiv 1 \pmod{5}$.

Osservazione 1.10. Quando un numero ammette inverso in congruenza, ne ammette infiniti; infatti, se a è l'inverso di $n \bmod m$, allora

$$n \cdot (a + km) \equiv n \cdot a + knm \equiv 1 + knm \equiv 1 \pmod{m}$$

Non sempre un numero ammette un inverso moltiplicativo per qualche modulo; di seguito, è riportata una condizione necessaria e sufficiente per l'esistenza dell'inverso.

Teorema 1.12

Un numero $a \in \mathbb{Z}$ ha inverso $\bmod m$ se e solo se $\gcd(a, m) = 1$.

Dimostrazione. Si assume che $\gcd(a, m) = 1$; per Bézout, si ha:

$$au + mv = 1$$

per qualche coppia $u, v \in \mathbb{Z}$. Questa uguaglianza, letta modulo m, diventa:

$$au \equiv 1 \pmod{m}$$

cioè u è inverso di $a \bmod m$.
Per l'implicazione inversa, si assume che a abbia inverso moltiplicativo u. Questo implica che $au \equiv 1 \pmod{m}$, che, a sua volta, diventa:

$$au - mk = 1$$

per qualche $k \in \mathbb{Z}$. Questo è sufficiente per affermare che $\gcd(a, m) = 1$. □

1.5.2 Congruenze lineari in una incognita

Si cercano le soluzioni x alla congruenza $ax \equiv b \pmod{m}$. Si inizia col notare che se $\exists d \in \mathbb{Z}$ tale che $d|a$ e $d|m$, ma $d \nmid b$ allora l'equazione non ha soluzioni.

Dimostrazione. Se per assurdo ne avesse almeno una $\overline{x}$, allora sarebbe soddisfatta $a\overline{x} - b = qm$, per qualche $q \in \mathbb{Z}$. Ma, nonostante m sia divisibile per d, l'altro membro non risulta tale per via di b, il che è assurdo. □

Da quanto appena notato, si conclude la condizione necessaria perché esista almeno una soluzione, ossia $\gcd(a, m)|b$.

Osservazione 1.11. Se $k|a, b$, allora l'equazionoe

$$\frac{a}{k}x \equiv \frac{b}{k} \mod \frac{m}{\gcd(k,m)}$$

è equivalente a $ax \equiv b \pmod{m}$, cioè hanno le stesse soluzioni. Si nota in particolare che, se s è un numero primo, allora l'equazione $sax \equiv sb \pmod{m}$ ha stesse soluzioni di quella di partenza.

Teorema 1.13

La congruenza $ax \equiv b \pmod{m}$ ha soluzione se e soltanto se $\gcd(a,m)|b$. Inoltre, il numero totale di soluzioni è $\gcd(a,m)$: le altre si ottengono sommandogli un multiplo di m.

Dimostrazione. La prima parte si è già dimostrata, quindi si dimostra solo quella relativa al numero di soluzioni. Assumendo che effettivamente $\gcd(a,m)|b$, allora $\gcd(a,m)$ è il massimo divisore comune di a, b, m; allora, dividendo la congruenza per questo, si ha:

$$a'x \equiv b' \pmod{m'}$$

dove

$$a' = \frac{a}{\gcd(a,m)} \qquad b' = \frac{b}{\gcd(a,m)} \qquad m' = \frac{m}{\gcd(a,m)}$$

dove a' e m' sono coprimi per costruzione. Essendo coprimi, significa che a' ha inverso moltiplicativo mod m'; sia questo e', il quale soddisfa $a'e' \equiv 1 \pmod{m'}$. Si può guardare la relazione dal punto di vista per cui l'inverso moltiplicativo di e' è a' e e' è coprimo con m'; in questo modo, si può moltiplicare per e' senza modificare il modulo:

$$e'a'x \equiv x \equiv e'b' \pmod{m'}$$

quindi le soluzioni dell'equazione sono tutte e sole quelle della forma

$$x = e'b' + qm' = e'b' + \frac{q}{\gcd(a,m)}m$$

per qualche $q \in \mathbb{Z}$. Questa forma permette di notare che esistono esattamente $\gcd(a,m)$ interi che risolvono questa equazione che non sono multipli di m. □

1.5.3 Il piccolo teorema di Fermat

Teorema 1.14 (Il piccolo teorema di Fermat)

Sia $p \in \mathbb{Z}$ un numero primo e $a \in \mathbb{Z}$ tale che $a \not\equiv 0 \pmod{p}$, cioè a non è multiplo di p[a]; allora

$$a^{p-1} \equiv 1 \pmod{p}$$

Dimostrazione. Per assunzione, $a \not\equiv 0 \pmod{p}$, quindi i numeri

$$a,\ 2a, \ldots, (p-1)a$$

sono, a due a due, non congrui mod p fra di loro; infatti, se così non fosse ed esistessero due numeri $i, j : 1 \leq i < j \leq p-1$ tali per cui $ia \equiv ja \pmod{p}$, allora $(i-j)a = qp$ per $q \in \mathbb{Z}$. Questo significa che, essendo a e p coprimi, per cui a ha inverso moltiplicativo b: $iab \equiv jab \pmod{m} \Rightarrow i \equiv j \pmod{m}$; questo non è possibile perché i e j erano stati assunti diversi e compresi tra 1 e $p-1$, quindi non possono avere stesso resto se divisi per p.
Allora, i resti dalla divisione per p di questi numeri sono nell'insieme $\{1, 2, \ldots, p-1\}$ perché il resto deve essere strettamente compreso da 1 e $p-1$ e deve essere diverso per ciascuno di quei numeri, per quanto appena mostrato. Questo permette di scrivere la seguente congruenza:

$$a \cdot (2a) \cdot \ldots \cdot \Big((p-1)a\Big) \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}$$

Raccogliendo a sinistra tutti i fattori a:

$$a^{p-1} \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}$$

Visto che ciascuno dei numeri è coprimo con p perché sono strettamente minori di p, si può moltiplicare questa congruenza per il loro inverso e arrivare a

$$a^{p-1} \equiv 1 \pmod{p}$$

□

[a] Questo basta per affermare che i due sono coprimi.

Corollario 1.3

Se $p \in \mathbb{Z}$ è primo, allora $\forall a \in \mathbb{Z}$ vale

$$a^p \equiv a \pmod{p}$$

Dimostrazione. Nel caso $a \not\equiv 0 \pmod{p}$, allora vale $a^{p-1} \equiv 1 \pmod{p}$ per il teorema di Fermat; usando ancora che a e p sono coprimi, si ottiene direttamente per moltiplicazione $a^p \equiv a \pmod{p}$.
Nel caso in cui $a \equiv 0 \pmod{p}$, invece, anche $a^p \equiv 0 \pmod{p}$; quindi, per transitività, si ha $a^p \equiv a \pmod{p}$. □

Corollario 1.4

Se $n \in \mathbb{Z}^{>1}$ è un intero tale che, per qualche $a \in \mathbb{Z}$, si ha $a^n \not\equiv a \pmod{n}$, allora n non è primo.

Osservazione 1.12. I numeri $n \in \mathbb{Z}^{>1}$ che soddisfano $a^n \equiv a \pmod{n}$ non sono necessariamente primi; questi sono noti come *falsi primi* e sono detti *numeri di Carmichael*.

1.6 Il teorema cinese del resto e classi di resto

1.6.1 Il teorema cinese del resto

Stabilisce una condizione per risolvere sistemi di congruenze. Si vuole risolvere un sistema del tipo

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{cases} \tag{1.6.1}$$

La soluzione della prima è data $x = a + km_1,\ k \in \mathbb{Z}$; inserendolo nella seconda (considerando k come variabile), si ottiene $a + km_1 \equiv b \pmod{m_2}$, da cui

$$m_1 k \equiv b - a \pmod{m_2} \implies km_1 - k'm_2 = b - a$$

che si sa avere soluzione (per th. 1.9) se e soltanto se $\gcd(m_1, m_2) \mid b - a$.

Si cerca di capire come trovare tutte le soluzioni una volta concluso che tale sistema ne ammette. A tale proposito, si considera una soluzione particolare k_0 di $km_1 \equiv b - a \pmod{m_2}$; quindi $x_0 = a + k_0 m_1$ risolve il sistema di partenza in eq. 1.6.1:

$$\begin{cases} x_0 \equiv a \pmod{m_1} \\ x_0 \equiv b \pmod{m_2} \end{cases}$$

Sia x_1 un'altra soluzione di tale sistema; prendendo la differenza, si ottiene:

$$\begin{cases} x_0 - x_1 \equiv 0 \pmod{m_1} \\ x_0 - x_1 \equiv 0 \pmod{m_2} \end{cases}$$

Quindi la differenza tra le soluzioni è sia multiplo di m_1 che di m_2. Il più piccolo intero che soddisfa questa condizione è chiamato *minimo comune multiplo* di m_1 e m_2 e si indica con $\operatorname{lcm}(m_1, m_2)$. Tutto questo si riassume nel seguente teorema.

Teorema 1.15 (Teorema cinese del resto)

Sia dato il sistema

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{cases}$$

Questo sistema ammette soluzione $\iff \gcd(m_1, m_2) \mid b - a$; in questo caso, data

x_0 una soluzione, tutte le altre soluzioni del sistema sono della forma

$$x_0 + s \cdot \operatorname{lcm}(m_1, m_2),\ s \in \mathbb{Z}$$

Osservazione 1.13. Equivalentemente, si può scrivere che tutte le soluzioni del sistema sono le x tali che

$$x \equiv x_0 \pmod{\operatorname{lcm}(m_1, m_2)} \tag{1.6.2}$$

Si nota, infine, che esiste un'unica soluzione x tale che $0 \leq x < \operatorname{lcm}(m_1, m_2)$.

Quando i moduli delle equazioni sono primi fra loro, cioè dato il sistema

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{cases}$$

con $\gcd(m_1, m_2) = 1$, il sistema ammette sempre soluzione e ne esiste un'unica x_0 tale che $0 \leq x_0 \leq m_1 \cdot m_2$; tutte le altre sono i numeri della forma

$$x_0 + 1 \cdot m_1 \cdot m_2,\ q \in \mathbb{Z} \tag{1.6.3}$$

Il teorema cinese del resto è generalizzabile ed enunciabile nella sua forma più classica, che è la seguente.

Teorema 1.16 (Teorema cinese del resto classico)

Dato il sistema di congruenze

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

dove i moduli sono, a due a due, coprimi, cioè $\gcd(m_i, m_j) = 1,\ \forall i \neq j$. Il sistema ammette sempre soluzione ed esiste un'unica soluzione x_0 tale che $0 \leq x_0 < m_1 \cdot \ldots \cdot m_n$. Tutte le altre soluzioni sono numeri della forma

$$x_0 + q \cdot m_1 \cdot \ldots \cdot m_n,\ q \in \mathbb{Z}$$

Dimostrazione. Si mostra a partire dal caso di un sistema di due congruenze, procedendo per induzione. □

1.6.2 Classi di resto

I possibili resti della divisione euclidea per 10 sono $0, 1, 2, \ldots, 9$; ad esempio, i numeri che danno resto 1 sono $1, 11, 21, 31, \ldots, -9, -19, 29, \ldots$ e si indica con $[1]_{10}$ l'insieme di tutti questi numeri, cioè:

$$[1]_{10} = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{10}\} \tag{1.6.4}$$

In generale, si indica con $[i]_{10}$ l'insieme degli interi che danno i come resto da divisione euclidea per 10. Gli insiemi per $i = 0, \ldots, 9$ si chiamano *classi di resto modulo 10* e la loro unione coincide con $\mathbb{Z}$. L'insieme i cui elementi sono le classi di resto modulo 10 si indica con

$$\mathbb{Z}_{10} = \{[0]_{10}, [1]_{10}, \ldots, [9]_{10}\} \tag{1.6.5}$$

Su questo insieme, si possono definire una somma e una moltiplicazione, ma prima è necessario estendere la notazione sviluppata finora perché al momento $[11]_{10}$ non è ben definito. Si sceglie di prendere $[11]_{10} = [1]_{10}$, o anche $[127]_{10} = [7]_{10}$ e, più in generale, $[s]_{10} = [i]_{10}$ qualora $s \equiv i \pmod{10}$.

In questo modo, la somma e il prodotto di elementi di $\mathbb{Z}_{10}$ sono definiti come:

$$\begin{aligned} [a]_{10} \cdot [b]_{10} &= [ab]_{10} \\ [a]_{10} + [b]_{10} &= [a+b]_{10} \end{aligned} \tag{1.6.6}$$

Esempio 1.2. Si ha:

$$\begin{aligned} [7]_{10} \cdot [5]_{10} &= [35]_{10} = [5]_{10} \\ [6]_{10} + [8]_{10} &= [14]_{10} = [4]_{10} \end{aligned}$$

In realtà, la verifica di avere definiti una buona somma e una buona moltiplicazione richiede la verifica che se $[a]_{10} = [a']_{10}$, $[b]_{10} = [b']_{10}$, allora

$$\begin{aligned} [a]_{10} \cdot [b]_{10} &= [a']_{10} \cdot [b']_{10} \\ [a]_{10} + [b]_{10} &= [a']_{10} + [b']_{10} \end{aligned}$$

Dimostrazione. DA DIMOSTRARE! *Suggerimento:* da $[a']_{10} = [a]_{10} \Rightarrow a' = a + 10k$ per qualche k e l'analogo vale per b'. Per la moltiplicazione, per esempio:

$$[a']_{10} \cdot [b']_{10} = [(a+10k)(b+10t)]_{10} = [ab + 10bk + 10at + 100kt]_{10} = [ab]_{10} = [a]_{10} \cdot [b]_{10}$$

□

Con queste operazioni, $\mathbb{Z}_{10}$ è un anello commutativo con unità; si nota che tali operazioni soddisfano la proprietà commutativa, associativa, distributiva, esistenza dell'elemento neutro e dell'opposto rispetto alla somma, eccetera. Una novità, invece, è che

$[2]_{10} \cdot [5]_{10} = [10]_{10} = [0]_{10}$, cioè il prodotto di due numeri non-nulli può fare zero: in questo caso, ad esempio, si dirà che $[2]_{10}, [5]_{10}$ sono divisori dello zero in $\mathbb{Z}_{10}$.

Questo discorso si può generalizzare per $m \in \mathbb{Z}^+$, cioè per $i = 0, 1, \ldots, m-1$, si definisce la classe di resto $[i]_m = \{x \in \mathbb{Z} \mid x \equiv i \pmod{m}\}$. Come nel caso $m = 10$, le classi di resto forniscono una partizione di $\mathbb{Z}$, cioè sono a due a due disgiunte e la loro unione restituisce proprio $\mathbb{Z}$. Si indica con $\mathbb{Z}_m$ o $\mathbb{Z}/m\mathbb{Z}$ l'insieme di queste classi:

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\} \tag{1.6.7}$$

che ha, dunque, cardinalità m. In modo del tutto analogo, si prende $[i]_m = [s]_m$ qualora $s \equiv i \pmod{m}$ e si definiscono le operazioni

$$[a]_m \cdot [b]_m = [a']_m \cdot [b']_m$$
$$[a]_m + [b]_m = [a']_m + [b']_m$$

Verificando come nel caso precedente che sono ben definite, si ottiene che $\mathbb{Z}_m$ è un anello commutativo con unità.

Osservazione 1.14. Il piccolo teorema di Fermat si può esprimere in modo equivalente tramite le classi di resto: dato p primo e la classe $[a]_p$ in $\mathbb{Z}_p$, con $[a]_p \neq [0]_p$, vale:

$$\left([a]_p\right)^{p-1} = [1]_p \tag{1.6.8}$$

Tramite questa osservazione, si vede che esiste un intero minimo $b \in \mathbb{Z}^+$ tale che $[a]_p^b = [1]_p$, con $b \leq p-1$; in questo caso, b sarà l'ordine moltiplicativo di $[a]_p$ in $\mathbb{Z}_p$. Questo b ha la proprietà per cui se $m \in \mathbb{Z}^+$ tale che $[a]_p^m = [1]_p$, allora $b|m$; in particolare, $b|p-1$.

Dimostrazione. Per vederlo, si usa la divisione euclidea per scrivere $m = qb + r$ e si ricava che $[a]_p^r = [1]_p$; a questo punto, si vede che deve essere $r = 0$ altrimenti verrebbe contraddetta la minimalità di b. □

1.7 La funzione di Eulero

Definizione 1.9 (Funzione di Eulero)

La funzione ϕ di Eulero è definita come

$$\phi : \mathbb{N}^{>0} \to \mathbb{N}^{>0} \qquad \phi(n) = \#\{a \leq n \mid \gcd(a, n) = 1\}$$

ossia rappresenta il numero degli interi positivi minori o uguali ad n che sono anche coprimi con n stesso.

Tramite questa, si enuncia un teorema che è la generalizzazione del piccolo teorema di Fermat.

Teorema 1.17

Sia $m \in \mathbb{Z}^{>0}$ e $a \in \mathbb{Z}$ tale che $\gcd(a,m) = 1$; allora

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Dimostrazione. Se $m = 1$, è ovvio perché tutti i numeri sono congrui fra loro modulo 1. Si può assumere, allora, $m \geq 2$ e si considerano le classi di resto $[a^0], [a^1], \ldots$; visto che queste sono le classi di resto modulo m, devono essere tutte diverse fino a un certo k, che è il più piccolo numero per cui una classe di resto si ripete: $[a^j] = [a^k] \Rightarrow j = 0$, altrimenti $[a^{j-1}] = [a^{k-1}]$ che è assurdo perché k era il più piccolo. Quindi $[a^k] = [a^0]$, cioè $a^k \equiv 1 \pmod{m}$. Si nota che se a è coprimo con m, allora anche tutte le sue potenze lo sono, il che vuol dire che le classi di resto distinte sono, al massimo, tante quante $\phi(m)$, cioè $k \leq \phi(m)$.
Se $k = \phi(m)$, il teorema è dimostrato. Si assume, altrimenti, che sia $k < \phi(m)$ e che sia $b < m$ un intero coprimo con m tale che $[b] \notin \left\{[a^0], [a^1], \ldots, [a^{k-1}]\right\}$; allora gli elementi $[ba^0], \ldots, [ba^{k-1}]$ sono tutti distinti fra loro e dai precedenti perché, essendo b corpimo con m per assunzione, se fosse $[ba^s] = [ba^t]$ per qualche $0 \leq s, t < k$, si avrebbe $[a^s] = [a^t]$ per le regole di divisione delle congruenze, da cui $s = t$. Invece, se fosse $[ba^s] = [a^t]$ per s, t come prima, moltiplicando per a^{k-s} (che è sempre coprimo con m), si ottiene $[b] = [a^{k-s+t}]$, il che è assurdo per costruzione di b.
In questo modo, si hanno $2k$ elementi distinti fra le $\phi(m)$ classi di resto coprime con m; se $\phi(m) = 2k$, il teorema è dimostrato, altrimenti si ripete il procedimento finché non si esauriscono le classi di resto, ottenendo $kd = \phi(m)$ per qualche intero $d > 0$. A questo punto:

$$a^{\phi(m)} \equiv a^{kd} \equiv (a^k)^d \equiv 1^d \equiv 1 \pmod{m}$$

che dimostra il teorema. □

Osservazione 1.15. Si nota che per $m = p$ primo, si ritrova l'enunciato del piccolo teorema di Fermat, visto che $\phi(p) = p - 1$.

Vista l'importanza della funzione ϕ, si cerca un modo per poterla calcolare efficacemente.

Definizione 1.10 (Funzione aritmetica moltiplicativa)

Una funzione $f : \mathbb{N}^{>0} \to \mathbb{N}^{>0}$ si dice *aritmetica moltiplicativa* se $\forall a, b \in \mathbb{Z}$: $\gcd(a,b) = 1 \Rightarrow f(ab) = f(a)f(b)$.

Proposizione 1.3

La funzione di Eulero ϕ è aritmetica moltiplicativa.

Dimostrazione. Si nota, preliminarmente, che dati s, t, m interi, con $m > 0$, tali

che $s \equiv t \pmod{m}$, si ha che s è coprimo con m se e solo se lo è t, visto che la congruenza è una relazione di equivalenza.
Sia, ora, $u \in \mathbb{Z}^{>0}$ coprimo con ab e $u < ab$; allora u è, in particolare, coprimo sia con a che con b, quindi risolve un sistema del tipo

$$\begin{cases} x \equiv v \pmod{a} \\ x \equiv w \pmod{b} \end{cases}$$

con $v \in \mathbb{Z}^{>0}$ coprimo con a e $v < a$ e $w \in \mathbb{Z}^{>0}$ coprimo con b e $w < b$. Viceversa, per il teorema cinese del resto, ogni sistema del genere ha una sola soluzione intera positiva minore di ab e, essendo coprima con a e con b, lo è anche con ab. Quindi i numeri interi positivi coprimi con ab e minori di ab sono tanti quanti i sistemi della forma di quello sopra, che sono $\phi(a)\phi(b)$, cioè il prodotto delle possibili scelte di v e w. □

Teorema 1.18

Sia $m \in \mathbb{Z}^{>0}$; se $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ è la sua decomposizione in fattori primi, allora:

$$\phi(m) = \left(p_1^{a_1} - p_1^{a_1-1}\right) \cdots \left(p_k^{a_k} - p_k^{a_k-1}\right)$$

Dimostrazione. Dalla proposizione precedente, si sa che $\phi(m)$ è il prodotto dei $\phi(p_i^{a_i})$; si deve, dunque, capire quanto vale $\phi(p^n)$, con p numero primo. Si nota che gli interi positivi minori di p^n sono tutti primi con p^n, tranne quelli che sono multipli di p; tuttavia, i multipli di p minori di p^n sono proprio p^{n-1}, quindi $\phi(p^n) = p^n - p^{n-1}$. □

Esempio 1.3. Con la teoria finora sviluppata, si può calcolare subito la classe di resto di 2^{365} modulo 225; visto che $\phi(225) = (25-5)(9-3) = 120$, per il teorema 1.17, si ha:

$$2^{120} \equiv 1 \pmod{225}$$

quindi

$$2^{365} \equiv (2^{120})^3 \cdot 2^5 \equiv 2^5 \equiv 32 \pmod{225}$$

Si nota che $\phi(m)$ non è il minimo intero che soddisfa il teorema 1.17; infatti, per questo teorema, si ha $2^8 \equiv 1 \pmod{15}$, ma, d'altra parte, vale anche $2^4 \equiv 1 \pmod{15}$. Questo si ha perché 1^n è congruo a 1 modulo m per qualunque n; inoltre, se $m > 2$, si ha $\phi(m) \neq 1$.

2 Teoria dei gruppi

2.1 Introduzione

Definizione 2.1 (Gruppo)

Un *gruppo* G è un insieme su cui è definita una *legge di composizione* $* : G \to G$ che soddisfa le seguenti condizioni per gli elementi di G:

GR 1. $(x * y) * z = z * (y * z)$ (*associatività*);

GR 2. $\exists e \in G : x * e = e * x = x$ (elemento neutro);

GR 3. $\forall x \in G$, $\exists y \in G$ tale che $x * y = y * x = e$ (elemento inverso).

Quando $*$ è la moltiplicazione, G si dice **gruppo moltiplicativo**; quando $*$ è l'addizione, G si dice **gruppo additivo**.

Definizione 2.2 (Gruppo commutativo)

Un insieme G è detto *gruppo commutativo* se è un gruppo e se soddisfa ulteriormente

$$x * y = y * x,\ \forall x, y \in G$$

L'elemento neutro di ciascun gruppo è unico.

Dimostrazione. Sia e' un altro elemento neutro; si nota che: $e = ee' = e'$. □

L'elemento inverso di ciascun elemento di un gruppo G è unico.

Dimostrazione. Siano y, y' gli elementi inversi di x; allora: $e = xy \implies y'e = y'xy \Rightarrow y' = y$. □

Questo elemento inverso si indica con x^{-1}; per gruppo additivo, si indicherà con $-x$.

Esempio 2.1. I numeri reali $\mathbb{R}$ e i numeri complessi $\mathbb{C}$ sono entrambi gruppi additivi. I numeri reali diversi da 0, $\mathbb{R}^*$, e i numeri complessi diversi da 0, $\mathbb{C}^*$, sono gruppi moltiplicativi.

Esempio 2.2. L'insieme dei numeri complessi di modulo 1, $\mathcal{S} := \{z \in \mathbb{C} : |z| = 1\}$, è un gruppo moltiplicativo.

Definizione 2.3 (Prodotto diretto)

Siano $G_1, \ldots, G_n$ dei gruppi; si definisce *prodotto diretto* l'insieme

$$G_P = \prod_{i=1}^{n} G_i = G_1 \times G_2 \times \ldots \times G_n$$

e contiene tutte le n-uple $(x_1, \ldots, x_n)$, $x_i \in G_i$.

Prendendo un prodotto diretto di gruppi ed equipaggiandolo con il prodotto componente per componente, dove l'elemento unità è $(e_1, \dots, e_n)$, con e_i unità di G_i, si ottiene un gruppo moltiplicativo.

Definizione 2.4 (Gruppo finito)

Un gruppo G si dice *finito* se ha un numero limitato di elementi; si chiama **ordine** il numero di elementi di tale gruppo e si indica con $|G|$.

Definizione 2.5 (Sottogruppo)

Sia G un gruppo e $H \subset G$ un sottoinsieme di G. Si dice che H è un sottogruppo di G se:

- $e \in H$;
- $\forall x, y \in H,\ x * y \in H$;
- $\forall x \in H,\ x^{-1} \in H$.

Definizione 2.6 (Generazione di un sottogruppo)

Sia $S = \{x_1, \dots, x_n\} \subset G$ un sottoinsieme di un gruppo G; l'insieme $H := \{x \in G : x = x_1 * \dots * x_n\} \cup \left\{x^{-1} \in G : x \in S\right\} \cup \{e \in G\}$ è un sottogruppo di G ed è detto *generato* da S, dove gli elementi di S sono detti i *generatori di* H.
In questo caso, si scriverà che $H = \langle S \rangle \equiv \langle x_1, \dots, x_n \rangle$.

Esempio 2.3. Si nota che $\{1\}$ è un generatore per il gruppo additivo degli interi, visto che ogni $z \in \mathbb{Z} \setminus \{0\}$ si può scrivere come $1 + 1 + \dots + 1$, o $-1 - 1 - \dots - 1$, mentre l'elemento neutro ne fa parte per definizione.

Definizione 2.7 (Centro di un gruppo)

Sia G un gruppo; si definisce il *centro di* G come l'insieme

$$Z(G) := \{g \in G \mid gh = hg,\ \forall h \in G\}$$

cioè è composto da tutti gli elementi di G che commutano con tutti gli altri elementi di G.

Proposizione 2.1

$Z(G)$ è un sottogruppo di G.

Dimostrazione. Intanto $e \in Z(G)$ perché l'unità rispetto all'operazione di G commuta con tutti gli altri elementi del gruppo; poi si nota che $Z(G)$ è chiuso sotto tale operazione perché se $h, k \in Z(G)$ e $g \in G$:

$$(hk)g = hgk = g(hk)$$

Infine, per $h \in Z(G)$, anche $h^{-1} \in Z(G)$ perché, dato $g \in G$:

$$g = h^{-1}hg = h^{-1}gh \iff [h^{-1}, g] = 0$$

□

Ora si definisce una notazione per indicare una ripetizione dell'operazione di composizione con lo stesso elemento. In generale, si scriverà:

$$x^n \equiv \underbrace{x * x * \ldots * x}_{n \text{ volte}} \tag{2.1.1}$$

Se $n = 0$, si definisce $x^n = e$; invece, se $n = -m$, si ha la seguente definizione:

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

Allora si possono verificare le seguenti:

- $x^{n+m} = x^n x^m$;
- $x^{-m}x^n = x^{n-m}$;
- $(x^n)^m = x^{nm}$.

Queste sono direttamente valide per la moltiplicazione, mentre per l'addizione si ha un qualcosa di analogo. Per cominciare $x^n \equiv nx$ nel caso dell'addizione, per definizione. Conseguentemente, le regole soddisfatte sono le seguenti:

$$(m+n)x = mx + nx \; ; \;\; (mn)x = m(nx)$$

Sia, G un gruppo e sia $a \in G$. Si definisce il sottogruppo H di G come quell'insieme avente tutti elementi del tipo a^n, $\forall n \in \mathbb{Z}$. In questo senso, H è generato da a. Per mostrare che è un gruppo, si nota che $e \in H$ perché $e = a^0$; dati, poi, $a^n, a^m \in H$, anche $a^{n+m} \equiv a^n a^m \in H$ perché $n + m \in \mathbb{Z}$. Infine, l'inverso di ciascun elemento a^n appartiene ad H perché $(a^n)^{-1} \equiv a^{-n}$, che appartiene ad H perché $-n \in \mathbb{Z}$.

Definizione 2.8 (Gruppo ciclico)

Sia G un gruppo; si dice che G è *ciclico* se esiste $a \in G : \forall g \in G,\ g = a^n$, per qualche intero n.

Riprendendo l'esempio 2.3, $\mathbb{Z}$ è un gruppo additivo ciclico, con generatore 1. Visto che un sottogruppo di Z è quello che si è chiamato *ideale*, si ha la seguente.

Proposizione 2.2

Sia H un sottogruppo di $\mathbb{Z}$. Se H non è il sottogruppo banale, sia d il più piccolo intero in esso contenuto; allora H contiene tutti elementi della forma nd, con $n \in \mathbb{Z}$, pertanto H è ciclico.

Sia G un gruppo ciclico e sia $a \in G$ il suo generatore; si hanno due casi possibili.

- *Caso 1*: non esiste $n \in \mathbb{Z}^{>0} : a^n = e$.

  Allora per ogni intero $n \neq 0$, $a^n \neq e$ e, allora, G si dice **infinitamente ciclico**, o che a ha **ordine infinito** perché ogni elemento $a^n \in G$ è distinto dall'altro.

  Dimostrazione. Si assume $a^r = a^s$ per qualche coppia di interi r, s; allora $a^{s-r} = e \Rightarrow s - r = 0 \Rightarrow r = s$. □

- *Caso 2*: $\exists m \in \mathbb{Z}^{>0} : a^m = e$.

  In questo caso, a ha **ordine finito**. Evidentemente, il gruppo è finito perché i suoi elementi si ripetono periodicamente.

  Sia J l'insieme degli $n \in \mathbb{Z}$ tali che $a^n = e$; allora J è un sottogruppo di $\mathbb{Z}$.

  Dimostrazione. Si ha $0 \in J$ perché $a^0 = e$ per definizione. Se $m, n \in J$, allora $a^{m+n} = a^m a^n = e \Rightarrow m + n \in J$. Infine, visto che $a^{-m} = (a^m)^{-1} = e$, anche $-m \in J$. □

Per il teorema 1.4, il più piccolo intero positivo contenuto in J genera J stesso; allora, per definizione, d è il più piccolo intero tale che $a^d = e$.

Definizione 2.9 (Periodo di un elemento)

Il più piccolo intero d tale che $a^d = e$ viene chiamato **periodo** di a. In quanto tale, se $a^n = e$ per qualche intero n, allora $n = ds$, per qualche intero s.

Teorema 2.1

Sia G un gruppo e sia $a \in G$ un elemento di periodo d; allora a genera il sottogruppo ciclico di ordine d, i cui elementi sono $e, a, \ldots, a^{d-1}$.

Dimostrazione. Per mostrare l'esistenza di tale sottogruppo, si nota che per $a \in G$, di periodo d, e per generico $n \in \mathbb{Z}$, l'algoritmo euclideo afferma che $n = qd + r$, con $q, r \in \mathbb{Z}$ e $0 \leq r < d$, per cui vale $a^n = a^r$.
Ora si mostra che gli elementi sono distinti. Se fosse $a^r = a^s$, con $0 \leq r, s \leq d - 1$ e, per assunzione, $r \leq s$, allora $a^{s-r} = e$; però $0 \leq s - r < d$, quindi bisogna avere $s - r = 0$, da cui $r = s$. □

2.2 Mappe tra gruppi

Dati S, S' due insiemi, una mappa fra questi è indicata con $f : S \to S'$; per $x \in S$, si indica con $f(x) \in S'$ l'immagine di x attraverso la mappa f. Per definire l'immagine di x attraverso f, si usa anche la notazione $x \mapsto f(x)$.

Data $f : S \to S'$ e $T \subset S$, si può definire una mappa che è la restrizione di f a T, assegnando $x \mapsto f(x)$, $\forall x \in T \subset S$; questa si indica con $f|_T : T \to S'$.

Una mappa $f : S \to S'$ si dice **iniettiva** se $\forall x, y \in S,\ x \neq y \Rightarrow f(x) \neq f(y)$. Una mappa si dice **suriettiva** se $\forall y \in S', \exists x \in S : f(x) = y$. Infine, f è **biettiva** se è sia iniettiva che suriettiva. Il fatto che f sia biettiva permette di individuare univocamente il suo inverso, la cui esistenza è assicurata dalla suriettività, mentre l'unicità dall'iniettività.

Definizione 2.10 (Mappa inclusione)

Sia S un insieme e $T \subset S$; la mappa identità di T, id_T, vista come mappa $\mathrm{id}_T : T \to S$ è chiamata *inclusione* e si indica con il simbolo $T \hookrightarrow S$.

Definizione 2.11 (Composizione)

Date due mappe $f : S \to T$, $g : T \to U$, si definisce la *mappa composta* come:

$$g \circ f : S \to U,\ (g \circ f)(x) = g\Big(f(x)\Big)$$

Va notato che la composizione *non* è commutativa[1], invece è, per definizione, associativa[2].

Proposizione 2.3

Siano S, T, U insiemi e siano $f : S \to T$, $g : T \to U$ due mappe; allora:

- f, g iniettive $\Rightarrow g \circ f$ iniettiva;
- f, g suriettive $\Rightarrow g \circ f$ suriettiva.

Definizione 2.12 (Mappa inversa)

Data $f : S \to S'$ una mappa; la sua inversa è la mappa $f^{-1} : S' \to S$ tale che

$$(f \circ f^{-1})(x') = \mathrm{id}_{S'};\ (f^{-1} \circ f)(x) = \mathrm{id}_S$$

Indicare l'inversa di f con f^{-1} presuppone che l'inversa sia unica, e infatti è così.

Dimostrazione. Sia $f : S \to S'$ e siano g_1, g_2 due mappe inverse per f; ma allora:

$$\mathrm{id}_{S'}(x') = (f \circ g_1)(x') \implies (g_2 \circ \mathrm{id}_{S'})(x') \equiv g_2 = g_2 \circ (f \circ g_1) = (g_2 \circ f) \circ g_1 \equiv g_1$$

□

Proposizione 2.4

Sia $f : S \to S'$; allora f è biettiva se e solo se f ha un'inversa.

Dimostrazione. Si divide la dimostrazione nelle due implicazioni.

- ($\Rightarrow$) Si assume che f sia biettiva e si mostra che ha un'inversa.

[1] se $f(x) = x^2$ e $g(x) = x + 1$, si ha $g \circ f = x^2 + 1$, mentre $f \circ g = (x+1)^2$.

[2] Infatti, se f, g, h sono tre mappe tali per cui $h(g(f(x))$ è ben definita, allora si ha $h \circ \Big(g \circ f\Big) = h \circ (g(f(x)) = h(g(f(x)))$, ma anche $(h \circ g) \circ f = (h \circ g)\Big(f(x)\Big) = h(g(f(x)))$.

La mappa f è tale che $\forall x' \in X', \exists! x \in X : f(x) = x'$; la mappa $x' \mapsto x$ è, allora, ben definita e questa coincide con l'inversa.

- ($\Leftarrow$) Si assume che f abbia un'inversa e si mostra che è biettiva.

  Per l'iniettività, si nota che se $x_1 \neq x_2$, allora deve essere anche $x_1' = f(x_1) \neq f(x_2) = x_2'$, altrimenti, se si avesse $f(x_1) = f(x_2) = x'$, $f^{-1}(x')$ non sarebbe una mappa ben definita perché ad un singolo elemento, ne fa corrispondere due.

  Per la suriettività, il discorso è analogo: $f^{-1} : S' \to S$ non sarebbe ben definita se si avesse $x_0' \in S' : \nexists x \in X,\ f(x) = x_0'$, allora non varrebbe $(f \circ f^{-1})(x_0') = \mathrm{id}_{S'}$.

□

Nonostante la precedente proposizione, la notazione f^{-1} si usa anche quando $f : X \to Y$ non ha propriamente un'inversa. In questo caso, f^{-1} è definita come una mappa tra l'insieme dei sottoinsiemi di Y e l'insieme dei sottoinsiemi di X. Così facendo, si rende possibile avere sempre una f^{-1} perché il suo risultato può essere l'insieme vuoto (nel caso in cui f non sia suriettiva), oppure un insieme composto da più elementi nel caso in cui f non sia iniettiva.

Definizione 2.13 (Sistemi di coordinate)

Siano gli $Y_1, \ldots, Y_n$ degli insiemi; si definisce sistema di coordinate una mappa

$$f : X \to \prod_{i=1}^{n} Y_i = Y_1 \times \ldots \times Y_n,\ f(x) = \Big(f_1(x), \ldots, f_n(x)\Big)$$

dove $f_i : X \to Y_i,\ i = 1, \ldots, n$.

2.3 Omomorfismi, isomorfismi e automorfismi

Definizione 2.14 (Omomorfismo)

Dati G, G' due gruppi, un omomorfismo $f : G \to G'$ è una mappa che conserva le operazioni di gruppo, cioè

$$\forall x, y \in G,\ f(x *_G y) = f(x) *_{G'} f(y)$$

con $*_G$, $*_{G'}$ leggi di composizione, rispettivamente, di G e G'.

Si ometteranno i pedici alle leggi di composizioni, ma la distinzione è sottintesa. Per brevità, invece di specificare che in $f : G \to G'$, G e G' sono gruppi, si dirà che $f : G \to G'$ è un *omomorfismo di gruppi*.

Esempio 2.4. Sia G un gruppo commutativo; allora la mappa $x \mapsto x^{-1} : G \to G$ è un omomorfismo. Si nota che la richiesta che G sia commutativo è fondamentale perché si abbia tale omomorfismo; infatti, $(x*y)^{-1} = x^{-1}*y^{-1}$ solamente se G è commutativo, altrimenti $x*y*(x*y)^{-1} = e \neq x*y*x^{-1}*y^{-1}$.

Esempio 2.5. La mappa $x \mapsto e^x : (\mathbb{R}, +) \to (\mathbb{R}^{>0}, \cdot)$ è un omomorfismo, infatti:

$$x + y \mapsto e^{x+y} = e^x \cdot e^y$$

Questo è un esempio in cui le leggi di composizione di gruppo sono diverse perché i due gruppi sono fondamentalmente diversi.

Proposizione 2.5

Siano G, H due gruppi, con $H = \prod_{i=1}^{n} H_i$. La mappa $f : G \to H$ è un omomorfismo se e soltanto se $\forall i,\ f_i$ è un omomorfismo.

Proposizione 2.6

Sia $f : G \to G'$ un omomorfismo di gruppi. Allora f conserva l'unità, nel senso che $f(e) = e'$, e conserva l'inversa, nel senso $f(x^{-1}) = f(x)^{-1}$.

Dimostrazione. Per la prima, si nota che $f(e) = f(ee) = f(e) * f(e)$. Moltiplicando (nel senso della legge $*_{G'}$) ambo i membri per $f(e)^{-1}$, si ottiene $e' = f(e)$.
Per la seconda, sia $x \in G$ tale che $\exists f^{-1}(x)$; allora $e' = f(x * x^{-1}) = f(x) * f(x^{-1})$.
Moltiplicando ambo i membri a sinistra per $f(x)^{-1}$, si ottiene $f(x)^{-1} = f(x^{-1})$. □

Si nota che nella proposizione di sopra, si è usata la notazione $f(x)^{-1}$ per indicare l'elemento inverso nel gruppo, ossia quell'elemento tale che $f(x) *_{G'} f(x)^{-1} = e'$, ben diverso da $f^{-1}(x)$ funzione inversa, tale che $f \circ f^{-1} = \mathrm{id}$.

Proposizione 2.7

Siano $f : G \to G'$, $g : G' \to G''$ due omomorfismi di gruppi; allora la loro composizione $g \circ f : G \to G''$ è un omomorfismo di gruppi.

Dimostrazione. Per calcolo diretto, si ha: $(g \circ f)(x*y) = g\Big(f(x*y)\Big) = g\Big(f(x)*f(y)\Big) = g\Big(f(x)\Big) * g\Big(f(y)\Big)$. □

Proposizione 2.8

Dato $f : G \to G'$ un omomorfismo di gruppi, l'immagine di f è un sottogruppo di G'.

Dimostrazione. Dati due elementi $f(x) = x',\ f(y) = y' \in \mathrm{Im}(f) \subset G'$, si ha:

$$x' * y' = f(x) * f(y) = f(x * y) \in \mathrm{Im}(f)$$

Quindi $\mathrm{Im}(f)$ è chiuso rispetto alla legge di composizione definita in G'. Anche

l'inverso appartiene a $\mathrm{Im}(f)$ perché $x^{-1} \in G \Rightarrow f(x)^{-1} = f(x^{-1}) \in \mathrm{Im}(f)$. Infine, anche l'identità vi appartiene sempre perché $e \in G \Rightarrow e' = f(e) \in \mathrm{Im}(f)$. □

Definizione 2.15 (Kernel di un omomorfismo)

Sia $f : G \to G'$ un omomorfismo di gruppi; il suo kernel (o nucleo) è l'insieme

$$\mathrm{Ker}(f) := \{x \in G : f(x) = e' \in G'\}$$

Proposizione 2.9

Il kernel di un omomorfismo di gruppi $f : G \to G'$ è un sottogruppo di G.

Dimostrazione. Se $x, y \in \mathrm{Ker}(f)$, allora $x*y \in \mathrm{Ker}(f)$ perché $f(x*y) = f(x)*f(y) = e'*e' = e'$. L'identità appartiene a $\mathrm{Ker}(f)$ perché $f(e) = e'$ e, per finire, se $x \in \mathrm{Ker}(f)$, anche x^{-1} vi appartiene perché $e' = f(e) = f(x * x^{-1}) = f(x) * f(x^{-1}) = e' * f(x^{-1}) \Rightarrow e' = f(x^{-1})$. □

Si considera, ora, un gruppo G e si prende un suo elemento $a \in G$; si nota che la mappa $n \mapsto a^n$ è un omomorfismo di $\mathbb{Z}$ in G. Questo è facile da dimostrare, ma più interessante è il fatto che il kernel di questo omomorfismo può essere composto o dal solo $0 \in \mathbb{Z}$, o è un sottogruppo generato dal periodo di a.

Proposizione 2.10

Sia $f : G \to G'$ un omomorfismo di gruppi; allora $\mathrm{Ker}(f) = \{e\}$ se e solo se f è iniettivo.

Dimostrazione. Si assume, quindi, che $\mathrm{Ker}(f) = \{e\}$ e si mostra che f è iniettiva. Dati $x, y \in G$, $x \neq y$, se per assurdo, si avesse $f(x) = f(y)$, allora $e' = f(x) * f(y)^{-1} = f(x * y^{-1}) \Rightarrow x * y^{-1} \in \mathrm{Ker}(f)$, con $x * y^{-1} \neq x * x^{-1} = e$ perché, per assunzione, $x \neq y$. Ne segue che f è iniettiva.
Il viceversa è banale perché se fosse $e \neq g \in \mathrm{Ker}(f)$, si avrebbe un assurdo dal momento che, per definizione di kernel, $f(g) = f(e) = e'$, dove e è l'unità di G ed e' è quella di G'. □

Un omomorfismo iniettivo fra due gruppi $G \to G'$ è chiamato **embedding** (o **iniezione**) e, come l'inclusione, si indica con $G \hookrightarrow G'$.

Proposizione 2.11

Sia $f : G \to G'$ un omomorfismo e sia $H' \subset G'$; prendendo $H = f^{-1}(H')$ come l'insieme delle $x \in G : f(x) \in H'$, allora H è un sottogruppo di G.

Si nota che nella proposizione sopra, per $H' = \{e'\}$, si ha $f^{-1}(H') \equiv \mathrm{Ker}(f)$.

Definizione 2.16 (Isomorfismo di gruppi)

Dato $f : G \to G'$ un omomorfismo di gruppi, si dice che è un *isomorfismo di gruppi* se esiste un altro omomorfismo di gruppi $g : G' \to G$ e tale che $f \circ g = \mathrm{id}_{G'}$ e $g \circ f = \mathrm{id}_G$. In tal caso, si dirà che $G \cong G'$.

Questo significa che se uno dei due ha delle proprietà esprimibili esclusivamente in termini delle operazioni di gruppo, allora anche ogni altro gruppo isomorfo a questo conserva le stesse proprietà. Alcune di queste sono:

- la ciclicità;
- l'ordine;
- l'essere abeliano.

Proposizione 2.12

Un omomorfismo di gruppi $f : G \to G'$ che è anche biettivo è un isomorfismo.

Dimostrazione. L'esistenza di $f^{-1} : G' \to G$ è assicurata dal fatto che f è biettiva. Si deve mostrare che f^{-1} è un omomorfismo.
Siano dati $x, y \in G' : f(x) = x',\ f(y) = y' \Rightarrow f(x * y) = x' * y'$, visto che f è un omomorfismo; allora si nota che:

$$f^{-1}(x' * y') = x * y = f^{-1}(x) * f^{-1}(y)$$

□

Dalla precedente proposizione, si ottiene il seguente teorema che permette di capire se un omomorfismo è un isomorfismo.

Teorema 2.2

Sia $f : G \to G'$ un omomorfismo di gruppi. Allora:

(a). se $\mathrm{Ker}(f) = \{e\} \implies f$ è un isomorfismo da $G \to f(G) \equiv \mathrm{Im}(f)$;

(b). $f : G \to G'$ è suriettiva e $\mathrm{Ker}(f) = \{e\}$, allora f è un isomorfismo da $G \to G'$.

Dimostrazione. Si è già dimostrato che se il nucleo di f è banale, allora f è iniettiva; chiaramente f è sempre suriettiva dall'insieme di partenza nella sua immagine, quindi la tesi è verificata dalla proposizione 2.12.
Sempre per la stessa, segue direttamente il punto (b). □

Definizione 2.17 (Automorfismo)

Un *automorfismo di gruppi* è un isomorfismo $f : G \to G'$ con $G' \equiv G$.

Si indica con $\mathrm{Aut}(G)$ l'insieme di tutti gli automorfismi definiti su G.

Definizione 2.18 (Traslazione)

Dato un gruppo G, la mappa che, per qualche $a \in G$, associa $x \mapsto a * x$, definita da $T_a : G \to G$, è chiamata *traslazione*. Questa, in particolare, è chiamata traslazione sinistra. La mappa inversa di una traslazione è $T_{a^{-1}}$, in quanto $x = a^{-1}ax$.

Si consideri la mappa che, per $a \in G$, associa $a \mapsto T_a : G \to \mathrm{Perm}(G)$; questa è un omomorfismo perché dati $a, b \in G$, si ha $T_{ab}(x) = abx = (T_a \circ T_b)(x)$, cioè $T_{ab} = T_a \circ T_b$. Evidentemente, questo isomorfismo è anche iniettivo perché per $a \neq b$, si ha $T_a \neq T_b$, pertanto $a \mapsto T_a$ risulta un isomorfismo su G, la cui immagine non è necessariamente coincidente con $\mathrm{Perm}(G)$.

Definizione 2.19 (Somma diretta)

Siano $B_1, \ldots, B_r$ dei sottogruppi di un gruppo abeliano additivo A; si dice che A è *somma diretta* di questi se

$$A = \bigoplus_{i=1}^{r} B_i = B_1 \oplus B_2 \oplus \ldots \oplus B_r$$

cioè se $\forall x \in A$, $x = \sum_{i=1}^{r} b_i$, $b_i \in B_i$ è scritto *univocamente* come somma di elementi dei B_i.

In generale, se A è un gruppo additivo abeliano, con B, C suoi sottogruppi, allora $B + C$ forma un sottogruppo di A, i cui elementi sono tutti della forma $b + c$, $b \in B$, $c \in C$.

Teorema 2.3

Sia A un gruppo abeliano; questo è somma diretta di suoi sottogruppi B, C se e soltanto se $A = B + C$ e $B \cap C = \{0\}$. Questo è vero se e soltanto se la mappa $(b, c) \mapsto b + c : B \times C \to A$ è un isomorfismo.

Per finire, si considera l'insieme degli omomorfismi tra due gruppi abeliani additivi A, B, indicato con $\mathrm{Hom}(A, B)$. È possibile rendere questo un gruppo, definendo $f + g : A \to B$, per $f, g \in \mathrm{Hom}(A, B)$, come

$$(f + g)(x) = f(x) + g(x), \ \forall x \in A$$

Dimostrazione. Si mostra che questo, così definito, è un gruppo. Intanto si osserva l'*associatività*:

$$\Big((f + g) + h\Big)(x) = (f + g)(x) + h(x) = f(x) + g(x) + h(x)$$
$$\Big(f + (g + h)\Big)(x) = f(x) + (g + h)(x) = f(x) + g(x) + h(x)$$

da cui $f + (g + h) = (f + g) + h$. Si ha anche l'elemento unità rispetto a $+$, indicato con 0, che ad ogni elemento di A, assegna l'elemento nullo di B, che risulta un omomorfismo.

Per finire, si definisce l'elemento $-f$ con la proprietà che $f+(-f)=0$ e si mostra che $f+g$ e $-f$ sono omomorfismi:

$$(f+g)(x+y)=f(x+y)+g(x+y)=f(x)+f(y)+g(x)+g(y)=(f+g)(x)+(f+g)(y)$$

e

$$(-f)(x+y)=-\Big(f(x+y)\Big)=-\Big(f(x)+f(y)\Big)=-f(x)-f(y)$$

Quindi $\mathrm{Hom}(A,B)$ è un gruppo. □

2.4 Permutazioni e gruppi simmetrici

Definizione 2.20 (Permutazione)
Sia S un generico insieme; è chiamata *permutazione* di S una mappa biettiva $f: S\to S$ e si indica con $\mathrm{Perm}(S)$ l'insieme delle permutazioni di S.

Le permutazioni dei numeri $1,2,\dots,n$ sono gli elementi di un gruppo, indicato con S_n, dove l'operazione è la legge di composizione di funzioni, come riportato di seguito.

Proposizione 2.13
L'insieme $\mathrm{Perm}(S)$ è un gruppo, la cui legge di composizione è data dalla composizione di mappe.

Dimostrazione. Si è già mostrato che la composizione di mappe è associativa e, chiaramente, esiste la permutazione identità che è id_S.
Inoltre, se f,g sono permutazioni, allora $g\circ f$, $f\circ g: S\to S$ e sono biettive, quindi sono permutazioni. Questo mostra che $\mathrm{Perm}(S)$ è chiuso sotto la composizione di mappe.
Infine, ogni permutazione f ha un'inversa f^{-1} perché f è biettiva per definizione. □

Questo risultato, più generale, afferma che l'insieme formato da qualunque permutazione su un insieme S è un gruppo, mentre i gruppi simmetrici S_n contengono solamente permutazioni dei primi n interi, cioè è il caso specifico di $S=\{1,\dots,n\}$. Generalmente, per la composizione di permutazioni, si scrive direttamente $\sigma\tau$, invece di $\sigma\circ\tau$.

Proposizione 2.14
Sia G un gruppo; l'insieme $\mathrm{Aut}(G)$, equipaggiato con la legge di composizione delle funzioni, è un sottogruppo di $\mathrm{Perm}(G)$.

Ora si caratterizzano le permutazioni nel caso del gruppo simmetrico S_n; una nota-

zione possibile è la seguente nel caso di $\tau \in S_9$:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 6 & 1 & 7 & 2 & 8 & 5 & 9 \end{pmatrix}$$

Tuttavia risulta ridondante perché basterebbe guardare la seconda riga, cioè invece di scrivere, per $\sigma \in S_n$

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

si può semplicemente scrivere $\sigma = \sigma(1)\sigma(2)\dots\sigma(n)$. Nel caso della permutazione τ scritta sopra, si avrebbe $\tau = 346172859$.

Un altro modo di rappresentare una permutazione è la *decomposizione in cicli disgiunti*:

$$\sigma = (1,3,6,2,4)(5,7,8)(9)$$

manda 1 in 3, 3 in 6, 6 in 2 e 4 in 1 e così via per i cicli successivi. In pratica, ogni elemento viene mandato in quello che lo segue, tranne l'ultimo che viene mandato nel primo (da qui "cicli"). L'ultimo ciclo afferma che il 9 viene mandato in se stesso, cioè viene lasciato fisso; in questi casi, è consuetudine non indicare elementi del genere, quindi la permutazione sopra si scriverebbe come $\sigma = (1,3,6,2,4)(5,7,8)$.

Si può dimostrare che ciascuna permutazione si può sempre scrivere come decomposizione di cicli disgiunti; il termine *disgiunti*, infatti, si riferisce proprio al fatto che all'interno di ciascun ciclo, un numero compare una sola volta. Inoltre, questa decomposizione non è unica; riprendendo l'esempio di $\sigma = (1,3,6,2,4)(5,7,8)$, questa è scrivibile anche come $\sigma = (5,7,8)(1,3,6,2,4) = (7,8,5)(6,2,4,1,3)$.

Definizione 2.21 (Trasposizione)

Si dice che τ è una trasposizione se è una permutazione che scambia due interi e lascia gli altri fissati. Questo significa che dati $i, j \in S_n : i \neq j \Rightarrow \tau(i) = j,\ \tau(j) = i$ e $\forall k \in S_n, k \neq i, j,\ \tau(k) = k$.

Si vede che se τ è una trasposizione, allora $\tau^2 = \mathrm{Id}$; inoltre, vale il seguente. Le trasposizioni sono permutazioni relative decomponibili in 2-cicli.

Teorema 2.4

Ogni permutazione di S_n si scrive come prodotto di trasposizioni.

Dimostrazione. Si procede per induzione su n. Per $n = 1$, non c'è nulla da provare. Si assume che questo sia vero in generale per $n > 1$ e, in particolare, per $n-1$, quindi si dimostra che vale per n. Sia σ una permutazione di S_n tale che $\sigma(n) = k$ e sia τ una trasposizione tale che $\tau(k) = n$ e $\tau(n) = k$; allora $\tau\sigma$ è una permutazione tale che $\tau\sigma(n) = \tau(k) = n$, cioè lascia n fissato. Questo vuol dire che può essere vista come permutazione di S_{n-1} che, per induzione, si può scrivere come

prodotto di trasposizioni $\tau_1, \dots, \tau_s \in S_{n-1}$: $\tau\sigma = \tau_1\tau_2\cdots\tau_s$. Conseguentemente, si ha $\sigma = \tau^{-1}\tau_1\cdots\tau_s$, che è un prodotto di trasposizioni in S_n. □

Esempio 2.6. Si considera S_{10}; date $\sigma = (1,3,6,2,4,7)(5,8,10)$ e $\tau = (1,3)(2,9)$, calcolare la decomposizione in cicli di $\tau\sigma$.

Svolgimento. La composizione delle due può essere calcolata notando preliminarmente che τ non modifica il ciclo $(5,8,10)$ di σ; in pratica, τ agisce unicamente su $(1,3,6,2,4,7)$[a]:

$$\begin{aligned}(1,3)(2,9)\circ(5,8,10)(1,3,6,2,4,7) &= (5,8,10)(2,4,7,3,6,9)(1)\\ &= (5,8,10)(2,4,7,3,6,9)\end{aligned}$$

■

[a] Si ricorda che i cicli vanno applicati da sinistra verso destra.

2.5 Classi di coniugio

Definizione 2.22 (Coniugazioni)

Sia G un gruppo e sia $a \in G$; si definisce *coniugazione* la mappa $\mathfrak{c}_a : G \to G$ tale che $x \mapsto axa^{-1}$.

Proposizione 2.15

$\mathfrak{c}_a$ è un automorfismo di G, in particolare, si definisce **automorfismo interno**. La mappa $a \mapsto \mathfrak{c}_a$ è un omomorfismo di $G \to \mathrm{Aut}(G)$, la cui legge di composizione è la composizione di funzioni.

Dimostrazione. Dato $g \in G$, si nota che $\mathfrak{c}_g$ è bigettiva perché ha un inverso dato da $\mathfrak{c}_{g^{-1}}$. Per mostrare che è un omomorfismo, quindi un automorfismo, si prendono $h,k \in G$ e si vede che:

$$\mathfrak{c}_g(hk) = ghkg^{-1} = ghg^{-1}gkg^{-1} = (ghg^{-1})(gkg^{-1}) = \mathfrak{c}_g(h)\mathfrak{c}_g(k)$$

□

Definizione 2.23 (Orbita rispetto al coniugio)

Dato G un gruppo e $\gamma \in G$, si definisce la *classe di coniugio* (o *orbita*) di γ l'insieme

$$\mathrm{Orb}(\gamma) = \left\{ g\gamma g^{-1} \mid g \in G \right\}$$

Le classi di coniugio formano una partizione di G, cioè ogni elemento di G appartiene ad una ed una sola classe di coniugio.

Dimostrazione. Si assume che esista un elemento comune ad entrambe le orbite $\mathrm{Orb}(\gamma_1)$

e $\mathrm{Orb}(\gamma_2)$, per esempio $g_1\gamma_1 g_1^{-1} = g_2\gamma_2 g_2^{-1}$. Da questo si ottiene che

$$\gamma_1 = (g_1^{-1}g_2)\gamma_2(g_2^{-1}g_1) = (g_1^{-1}g_2)\gamma_2(g_1^{-1}g_2)^{-1} = g'\gamma_2 g'^{-1} \iff \gamma_1 \in \mathrm{Orb}(\gamma_2)$$

Ma il fatto che $\gamma_1 \in \mathrm{Orb}(\gamma_2) \Rightarrow \mathrm{Orb}(\gamma_1) = \mathrm{Orb}(\gamma_2)$. Questo dimostra che ogni elemento di G può appartenere ad un'unica classe di coniugio, altrimenti due classi distinte coinciderebbero e sarebbero comunque una sola. □

Infatti, si può definire la relazione di equivalenza per cui $x \sim y \iff x = gyg^{-1}$ per $g \in G$, quindi il gruppo si partiziona sotto questa relazione di equivalenza.

Ora si studiano le classi di coniugio di S_n; per farlo, date le permutazioni σ e τ si usa la decomposizione in cicli:

$$\sigma = (a_1, a_2, \dots, a_{k_1})(b_1, b_2, \dots, b_{k_2})\cdots$$

Allora vale la seguente formula, utile per i calcoli:

$$\tau\sigma\tau^{-1} = \Big(\tau(a_1), \tau(a_2), \dots, \tau(a_{k_1})\Big)\Big(\tau(b_1), \dots, \tau(b_{k_2})\Big)\cdots \tag{2.5.1}$$

Esempio 2.7. Se $\sigma, \tau \in S_5$, con $\sigma = (1,3,5)(2,4)$ e $\tau = (1,2,4,5)$, allora

$$\tau\sigma\tau^{-1} = \Big(\tau(1), \tau(3), \tau(5)\Big)\Big(\tau(2), \tau(4)\Big) = (4,3,1)(5,2)$$

2.6 Classi laterali

Siano S, S' due sottoinsiemi di un gruppo $(G, *)$; il loro **prodotto** è:

$$S * S' = \{x \in G : x = s * s',\ s \in S,\ s' \in S'\}$$

Allora, se $S_1, S_2, S_3 \subset G$, vale $(S_1 * S_2) * S_3 = S_1 * (S_2 * S_3)$. Di seguito, alcune altre proprietà.

- Sia H sottogruppo di G; allora $H * H = H$.

  Dimostrazione. È sufficiente prendere l'elemento neutro di uno dei due e far variare tutti gli elementi dell'altro per ottenere tutto H. Non si può uscire da H perché H stesso è un gruppo, quindi è chiuso rispetto a $*$. □

- Sia $S \subset H$ un generico sottoinsieme e H come sopra; allora $S * H = H$.

  Dimostrazione. Corrisponde a traslare ciascun elemento di H, ma si riottiene comunque H. Per vederlo, sia $s \in S$ fissato; dato un generico $h_0 \in H$, si vuole mostrare che $\exists h \in H : s * h = h_0$.

Visto che H è un sottogruppo di G, H contiene l'inverso di qualunque suo elemento e di ogni elemento di S, pertanto è ben definito $h = s^{-1} * h_0$, che soddisfa la richiesta. □

- Dati $S_1, S_2, S_3 \subset G$, allora $S_1 * (S_2 \cup S_3) = S_1 * S_2 \cup S_1 * S_3$.

  Dimostrazione. Si indica con $S := S_1 * (S_2 \cup S_3)$ e con $\overline{S} := S_1 * S_2 \cup S_1 * S_3$.

  Un generico elemento di S è il prodotto tra $s_1 \in S_1$ e un altro elemento che sta in S_2 o in S_3. Un generico elemento di $\overline{S}$ è o il prodotto tra $s_1 \in S_1$ e $s_2 \in S_2$, o $s_1 \in S_1$ e $s_3 \in S_3$. Allora $S = \overline{S}$. □

Definizione 2.24 (Classe laterale)

Sia G un gruppo e sia H un suo sottogruppo. Dato $a \in G$, l'insieme di tutti gli elementi della forma ax, $x \in H$ è chiamato *classe laterale* di H in G.
Si indicherà con aH.

Si nota che, essendo in generale G non-commutativo, la scrittura $aH \neq Ha$; la prima si chiama *classe laterale sinistra*, mentre la seconda sarà la *classe laterale destra*.

Osservazione 2.1. Più precisamente dovrebbe essere $a * H$, ma si elimina $*$ per alleggerire la notazione. Nel caso della somma, diventerebbe $a + H$.

Teorema 2.5

Siano aH e bH due classi laterali di H in G: o le due classi laterali sono uguali, o non hanno alcun elemento in comune.

Dimostrazione. Si assume che $\exists x, y \in H : ax = by$. Allora si osserva che, essendo $xH = H = yH$:

$$aH = axH = byH = bH$$

□

È possibile decomporre un gruppo in classi laterali. Si considera il caso specifico di G gruppo finito; ogni elemento $x \in G$ appartiene ad una classe laterale, per esempio xH, con H sottogruppo di G. Allora, G si può scrivere come unione finita di classi laterali di H[1]:

$$G = \bigsqcup_{i=1}^{r} a_i H \tag{2.6.1}$$

dove ogni classe laterale è distinta dall'altra, altrimenti sarebbero uguali e non si sarebbe aggiunto nessun nuovo elemento di G. Ogni elemento ah, $h \in H$ è chiamato **rappresentante** della classe laterale aH.

[1] Il simbolo $\bigsqcup$ indica unione di insiemi disgiunti.

Lo stesso si può dire per gruppi infiniti, ma sono ammesse unioni di infinite classi laterali; indicando con I un certo insieme di indicizzazione potenzialmente infinito:

$$G = \bigsqcup_{i \in I} a_i H \tag{2.6.2}$$

con G finito o infinito.

Teorema 2.6

Sia G un gruppo e H un sottogruppo finito. Allora il numero di elementi di una certa classe laterale aH è il numero di elementi di H.

Dimostrazione. Siano $x, x' \in H : x \neq x'$; allora, $ax \neq ax'$ perché se fosse $ax = ax'$, si potrebbe moltiplicare ambo i membri per a^{-1} e ottenere $x = x'$, il che è falso per assunzione di partenza.
Ne segue che, prendendo $x_1, \ldots, x_n \in H$ tutti diversi, anche $ax_1, \ldots, ax_n$ sono diversi, quindi il numero di elementi di una classe coincide col numero di elementi di H. □

Dati G, H come al solito, si indica con G/H l'insieme di tutte le classi laterali sinistre di H in G. Si chiama **indice** il numero di tutte le distinte classi laterali di H in G e si indica con $(G : H)$. Se $|S|$ è il numero di elementi in S, allora $|(G/H)| = (G : H)$ e $|G| = (G : 1)$.

Teorema 2.7 (Teorema di Lagrange)

Sia G un gruppo finito e H un suo sottogruppo; allora

$$|G| = (G : H)|H|$$

Dimostrazione. Per teorema 2.5, ogni elemento di G sta in, esattamente, una classe laterale; se $g \in G \Rightarrow g \in gH$ perché $g * e \in gH$. Per teorema 2.6, ciascuna classe ha lo stesso numero di elementi.
La relazione segue direttamente da queste conclusioni perché ogni classe laterale contiene $|H|$ elementi distinti di G e diversi da tutte le altre che decompongono G stesso (altrimenti le classi sarebbero uguali), il cui numero è $(G : H)$. □

Corollario 2.1

Sia G un gruppo finito e H un suo sottogruppo; allora $|H|$ divide $|G|$.

Corollario 2.2

Sia G un gruppo e $a \in G$ un suo elemento; il periodo di a, divide $|G|$.

Dimostrazione. Il periodo di a è il numero di elementi del sottogruppo generato da a stesso. □

Corollario 2.3

Sia G un gruppo e siano $K \subset H \subset G$ due sottogruppi; allora $(G:K) = (G:H)(H:K)$.

Dimostrazione. Applicando due volte Lagrange:

$$|G| = (G:H)|H| = (G:H)(H:K)|K|$$

Allo stesso tempo, sempre per Lagrange, $|G| = (G:K)|K|$, quindi:

$$(G:K)|K| = (G:H)(H:K)|K| \implies (G:K) = (G:H)(H:K)$$

□

Si considera d'esempio il gruppo S_n delle permutazioni di $\{1,\dots,n\}$. Sia H il sottogruppo di S_n che contiene tutte le permutazioni σ della forma $\sigma(n) = n$; questo, come sottogruppo, coincide con $S_{n-1}, n > 1$. Si studiano le classi laterali di H; più in dettaglio, vale il seguente.

Proposizione 2.16

Le sole classi laterali distinte di $H \equiv S_{n-1},\ n > 1$ come sottogruppo di S_n sono

$$\tau_1 H, \dots, \tau_n H \tag{2.6.3}$$

con $\tau_i(n) = i,\ \tau_i(i) = n$ e tutti gli altri interi sono lasciati invariati.

Dimostrazione. Per prima cosa, si mostra che ogni elemento $\sigma \in S_n$ è contenuto in una classe laterale. Intanto si nota che H coincide con $\tau_n H$ perché τ_n è l'identità per definizione; allora, si prende un elemento che non sta in H e si mostra che appartiene ad una classe laterale. Senza perdita di generalità, quindi, sia $\sigma \in S_n$: $\sigma(n) = i$; allora

$$\tau_i^{-1} \circ \sigma(n) = \tau_i^{-1}(i) = n$$

Questo significa che $\tau_i^{-1}\sigma \in H \implies \sigma \in \tau_i H$. Questo dimostra che $S_n/H \equiv \{\tau_i H\}_{i=1}^n$; manca da mostrare che queste sono tutte distinte.
Per vederlo, si assume $i \neq j$ e si nota che, $\forall \sigma \in H$, $\tau_i \circ \sigma(n) = \tau_i(n) = i$ e $\tau_j \circ \sigma(n) = j$, quindi $\tau_i H$ e $\tau_j H$ non possono avere elementi in comune, □

Vista la proposizione 2.16, il teorema di Lagrange permette anche di concludere che $|S_n| = n|S_{n-1}|$; per induzione, si mostra che, in generale:

$$|S_n| = n! \tag{2.6.4}$$

Teorema 2.8

Sia $f : G \to G'$ un omomorfismo di gruppi. Dato $a' \in \mathrm{Im}(f) \subset G'$, con $a' = f(a)$ per qualche $a \in G$, allora l'insieme degli elementi $x \in G : f(x) = a'$ coincide con la

classe laterale $a\text{Ker}(f)$.

Dimostrazione. L'idea è di mostrare che i due insiemi sono contenuti uno nell'altro.
Sia $x \in a\text{Ker}(f)$, cioè per qualche $h \in \text{Ker}(f)$, $x = ah$; allora:

$$f(x) = f(a) * f(h) = f(a)$$

cioè $x \in a\text{Ker}(f) \implies x \in \{y \in G : f(y) = a'\}$.
Sia ora $x \in \{y \in G : f(y) = a'\}$; allora:

$$f(a^{-1}x) = f(a)^{-1} * f(x) = a'^{-1} * a' = e'$$

cioè $a^{-1}x \in \text{Ker}(f)$, per esempio $h = a^{-1}x$, quindi $x = ah \implies x \in a\text{Ker}(f)$. □

2.7 Sottogruppi normali

Definizione 2.25 (Sottogruppo normale)

Sia G un gruppo e sia H un suo sottogruppo. Si dice che H è *normale* se soddisfa una delle due, equivalenti, condizioni:

NOR 1. $\forall x \in G,\ xH = Hx$, cioè $xHx^{-1} = H$;

NOR 2. H è il kernel di qualche omomorfismo di G in qualche altro gruppo.

Per indicare che H è un sottogruppo normale di G si scrive $H \triangleleft G$.

Intanto si nota che la condizione NOR 1 non coincide con la condizione $xhx^{-1} = h,\ \forall h \in H$ quando G non è commutativo. Nel caso di G commutativo, ogni sottogruppo H è normale e soddisfa la condizione più forte di NOR 1, cioè proprio $x^{-1}hx = h,\ \forall h \in H$.

Ora si dimostra che NOR 1 $\iff$ NOR 2. L'implicazione NOR 1 $\implies$ NOR 2 si vede di seguito.

Dimostrazione. Sia $H \equiv \text{Ker}(f)$, con $f : G \to G'$ un omomorfismo di gruppi; allora:

$$f(xHx^{-1}) = f(x)f(H)f(x)^{-1} = e' \in G'$$

Da questo, segue che $xHx^{-1} \subset H,\ \forall x \in G$, quindi vale anche $x^{-1}Hx \subset H$[1], da cui (moltiplicando a sinistra per x e a destra per x^{-1}) si ha $H \subset xHx^{-1}$. □

L'altra implicazione si dimostra nel seguente teorema e nel successivo corollario.

[1] Visto che tale condizione vale $\forall x \in G$, si può mandare $x \to x^{-1}$ e, conseguentemente, $x^{-1} \to x$ e ottenere $x^{-1}Hx \subset H$.

Teorema 2.9

Sia G un gruppo e sia H un sottogruppo tale che $xH = Hx$, $\forall x \in G$. Se aH, bH sono due classi laterali di H, allora il prodotto $(aH) * (bH)$ è ancora una classe laterale. Inoltre, l'insieme delle classi laterali è esso stesso un gruppo, il cui prodotto è quello appena descritto.

Dimostrazione. La prima affermazione è immediata: $(aH) * (bH) = aHbH = abHH = abH$, usando che $xH = Hx$.
L'assioma GR 1 è osservata all'inizio di §2.6; GR 2 è soddisfatto da $eH = H$; GR 3, infine, è soddisfatto da $a^{-1}H$ come inverso di aH. □

Il gruppo delle classi laterali G/H è chiamato **gruppo quoziente** e si dice anche G **modulo** H. Il poter trattare questo come un gruppo è dovuto all'assunzione $xH = Hx$.

> **Osservazione 2.2.** Parlando di gruppo quoziente G/H si assumerà sempre che H è un sottogruppo normale di G.
> È chiaro che per essere vero che G/H è un gruppo quoziente, H deve per forza essere un sottogruppo normale di G, da qui il motivo per cui lo si sottintende.

Corollario 2.4 (Omomorfismo canonico)

Sia G un gruppo e sia H un sottogruppo normale. Sia G/H il gruppo quoziente e $f : G \to G/H$ la mappa che, ad ogni $a \in G$, associa la classe laterale aH, cioè $f(a) = aH$. Allora f è un omomorfismo e $\mathrm{Ker}(f) \equiv H$.

Dimostrazione. È evidente che f sia un omomorfismo dalla definizione di prodotto di classi laterali. Per il kernel, si vede che ogni elemento di H è automaticamente in $\mathrm{Ker}(f)$ perché se $h \in H \Rightarrow f(h) = hH \equiv H$. Sia, invece, $x \in G : f(x) = xH$ sia l'elemento unità di G/H, quindi coincidente con il laterale H stesso: $xH = H$. Questo vuol dire che $xe = x$ è un elemento di H. Quindi H coincide con il kernel di f. □

Sia $f : G \to G'$ un omomorfismo. Dato $x \in G$, allora, $\forall k \in \mathrm{Ker}(f)$:

$$f(xk) = f(x)f(k) = f(x) \implies f(x\mathrm{Ker}(f)) = f(x)$$

Questo significa che ogni elemento in un laterale di $\mathrm{Ker}(f)$ ha la stessa immagine sotto f.

Corollario 2.5

Sia $f : G \to G'$ un omomorfismo e sia $H = \mathrm{Ker}(f)$; allora la mappa $x\mathrm{Ker}(f) \mapsto f(x\mathrm{Ker}(f))$ è un isomorfismo del gruppo quoziente G/H con l'immagine di f, cioè $G/H \xrightarrow{\approx} \mathrm{Im}(f)$. In questo caso, si dice che l'isomorfismo $\overline{f}$ è **indotto** da f.

Dimostrazione. Si definisce $\overline{f} : G/H \to G'$ t.c. $xH \mapsto f(xH)$. Ora si verifica che è un

isomorfismo usando il teorema 2.2. Intanto si ha che $\overline{f}$ è un omomorfismo, infatti:

$$\overline{f}(xHyH) = \overline{f}(xyH) = f(xy) = f(x)f(y) = \overline{f}(xH)\overline{f}(yH)$$

È anche iniettiva perché il suo nucleo sono quei laterali xH tali che $f(xH) = e'$, quindi solamente H, che è l'unità di G/H. Infine si ha $\mathrm{Im}(\overline{f}) = \mathrm{Im}(f)$ per definizione di f. Quest'ultima considerazione permette di concludere che $G/H \cong \mathrm{Im}(f)$. □

Esempio 2.8. Si considera, come esempio, $\mathbb{Z}$ come sottogruppo del gruppo additivo $(\mathbb{R}, +)$; il gruppo quoziente $\mathbb{R}/\mathbb{Z}$ è chiamato **gruppo circolare**.
Dati due numeri reali $x, y \in \mathbb{R}$, si dice che $x \equiv y \pmod{\mathbb{Z}}$ se $x - y \in \mathbb{Z}$; questa definisce una relazione di equivalenza, le cui classi di equivalenza sono esattamente i laterali di $\mathbb{Z}$ in $\mathbb{R}$. Se è vero che $x \equiv y \pmod{\mathbb{Z}}$, allora $e^{2\pi i x} = e^{2\pi i y}$ e la mappa $x \mapsto e^{2\pi i x}$ definisce un isomorfismo di $\mathbb{R}/\mathbb{Z}$ nel gruppo moltiplicativo dei numeri complessi che hanno modulo unitario.

Esempio 2.9. Siano $\mathbb{C}^*$ e $\mathbb{R}^+$, rispettivamente, il gruppo moltiplicativo dei numeri complessi non-nulli e il gruppo moltiplicativo dei reali positivi.
Dato $\alpha \in \mathbb{C}^*$, vale $\alpha = ru$, con $r \in \mathbb{R}^+$ e $|u| = 1$ (si prende $u = \alpha/|\alpha|$). L'espressione di u è sempre determinata e la mappa $\alpha \mapsto \alpha/|\alpha|$ è un omomorfismo di $\mathbb{C}^*$ in $\mathbb{C}_1 := \{x \in \mathbb{C} : |x| = 1\}$. Essendo il nucleo di questo omomorfismo proprio $\mathbb{R}^+$, allora $\mathbb{C}^*/\mathbb{R}^+ \cong \mathbb{C}_1$.

Riprendere da pagina 48 dopo esempio 5