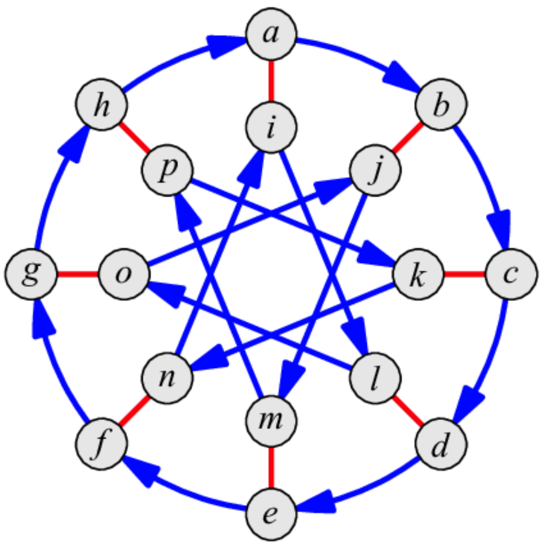
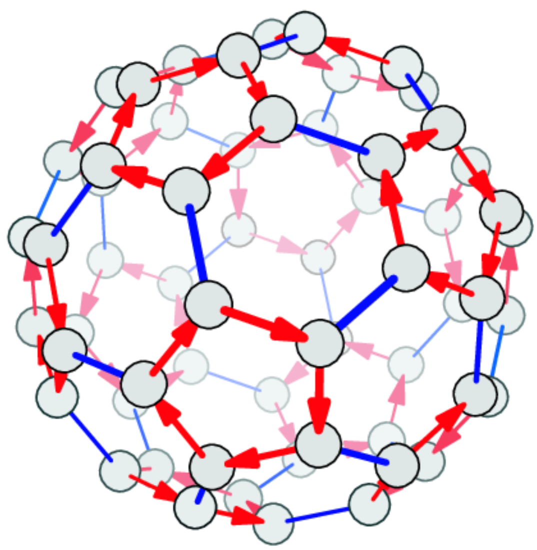
APPUNTI DI ALGEBRA

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 piÃź 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 relativamente primi)

Siano $m_1, \ldots, m_r$ degli interi il cui massimo comune divisore è 1. Allora $m_1, \ldots, m_r$ si dicono *relativamente primi* 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 relativamente primi 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 relativamente primo con se stesso, avendo come altro divisore se stesso 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. $\square$

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 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:

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

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 $\square$

[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 $p_i | q_1 \dots q_s$.

1.4 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. $\forall x \in S,\ x \sim x$;

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 n un intero positivo e siano x, y due interi. Si dice che x è *congruente y modulo n* se $\exists m : x - y = mn$. In tal caso, si scriverà $x \equiv y \pmod{n}$.

La congruenza di x, y come $x - y = mn$ implica automaticamente che $x - y$ appartiene all'ideale generato da n; inoltre, se $n \neq 0$, allora $x - y$ è divisibile per n.

Oltre alle proprietà delle relazioni di equivalenza, la congruenza ne soddisfa anche altre due:

- se $x \equiv y \pmod{n}$ e z è un intero, allora $xz \equiv yz \pmod{n}$;
- se $x \equiv y \pmod{n}$ e $x' \equiv y' \pmod{n}$, allora $xx' \equiv yy' \pmod{n}$[1] e $x + x' \equiv y + y' \pmod{n}$.

Dalla definizione di congruenza, si definiscono gli interi **pari** come quelli che sono congruenti a 0 (mod 2) (quindi $n = 2m$) e quelli **dispari** come gli interi che non sono pari, quindi della forma $2m + 1$, per qualche intero m.

[1]Per dimostrare questa, basta notare che $xx' - yy' = xx' + x'y - x'y - yy' = x'(x - y) + y(x' - y')$.

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, $\mathscr{I} := \{z \in \mathbb{C} : |z| = 1\}$, 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 $(e_1, \ldots, e_n)$, 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.

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 $S = \{x_1, \ldots, x_n\} \subset G$ un sottoinsieme di un gruppo G; l'insieme $H := \{x \in G : x = x_1 * \ldots * x_n\} \cup \left\{x^{-1} \in G : x \in S\right\} \cup \{e \in G\}$ 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 $H = \langle S \rangle \equiv \langle x_1, \ldots, x_n \rangle$.

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 $1 + 1 + \ldots + 1$, o $-1 - 1 - \ldots - 1$, mentre l'elemento neutro ne fa parte per definizione.

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:

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

2.1.1 Gruppi ciclici

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 2.7 (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 2.1

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 $a^{s-r} = e \Rightarrow s - r = 0 \Rightarrow r = s$. $\square$

- *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 $-m \in J$. $\square$

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 $a^d = e$ e, per questo, 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 $e, a, \dots, a^{d-1}$.

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 $r = s$. $\square$

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 2.8 (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 2.9 (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].

[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 $(h \circ g) \circ f = (h \circ g)\big(f(x)\big) = h(g(f(x)))$.

Proposizione 2.2

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 2.10 (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 2.3

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.
  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 2.11 (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.

Proposizione 2.4

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. □

Generalmente, per la composizione di permutazioni, si scrive direttamente $\sigma\tau$, invece di $\sigma \circ \tau$.

Definizione 2.12 (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 di gruppo

Definizione 2.13 (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 $f \circ f^{-1} = \text{id}$.

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: $(g \circ f)(x * y) = g\big(f(x * y)\big) = g\big(f(x) * f(y)\big) = g\big(f(x)\big) * g\big(f(y)\big)$. $\square$

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 $e \in G \Rightarrow e' = f(e) \in \mathrm{Im}(f)$. $\square$

Definizione 2.14 (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 $e' = f(e) = f(x * x^{-1}) = f(x) * f(x^{-1}) = e' * f(x^{-1}) \Rightarrow e' = f(x^{-1})$. $\square$

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; se $\mathrm{Ker}(f) = \{e\}$, allora 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. $\square$

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.

Dimostrazione. DA DIMOSTRARE. $\square$

Riprendere da metà pagina 35.