CAPITOLO QUARTO

I GRUPPI

1 Definizione di gruppo.

Definizione 1. *Un* **gruppo** *è una coppia (G,μ), dove G è un insieme e μ è una* **legge di composizione**, *ossia un'applicazione $\mu : G \times G \longrightarrow G$ che associa ad ogni coppia (x, y) di $G \times G$ un elemento di G che indicheremo con xy, e che soddisfa le seguenti proprietà:*

1. **Associatività**: *per ogni $x, y, z \in G$ $(xy)z = x(yz)$.*
2. **Identità sinistra:** *esiste un $e \in G$ tale che per ogni $x \in G$ $ex = x$.*
3. **Reciproco sinistro:** *per ogni $x \in G$ esiste almeno un $y \in G$ tale che $yx = e$.*

La legge $(x, y) \longrightarrow xy$ si chiama di solito **moltiplicazione**, l'elemento xy è il prodotto di x e y.

Parleremo del "gruppo G" sottintendendo la legge μ.

Come conseguenza della proprietà associativa si può scrivere xyz in luogo di $(xy)z$. Analogamente si scriverà $xyzwv, ...$

Lemma 1. *Sia G un gruppo. Allora:*

1. *esiste un* unico *$e \in G$ (detto l'* **identità** *di G tale che $ex = x$ per ogni $x \in G$; si ha inoltre che $xe = x$ per ogni $x \in G$;*
2. *per ogni $x \in G$ esiste un unico $x^{-1} \in G$ (detto il* **reciproco** *o l'* **inverso** *di x, e sempre indicato con x^{-1}) tale che $x^{-1}\, x = e$; ed allora $x\, x^{-1} = e$;*
3. *per ogni $x \in G$ risulta $(x^{-1})^{-1} = x$*
4. *per ogni $x, y \in G$ risulta $(xy)^{-1} = y^{-1}\, x^{-1}$.*

Dimostrazione.

1. Proprietà $xe = x$:
   $xe = xx^{-1}x = ex = x$

2. Dimostrazione della proprietà $xx^{-1} = e$: si noti che x^{-1}, eventualmente non unico, esiste come conseguenza della definizione di gruppo; si ha allora

   $x^{-1}xx^{-1} = ex^{-1} = x^{-1}$,

   e moltiplicando a sinistra del primo membro per un reciproco $(x^{-1})^{-1}$ di x^{-1} si ha

   $(x^{-1})^{-1}x^{-1}xx^{-1} = exx^{-1} = xx^{-1}$

   a sinistra del secondo membro:

   $(x^{-1})^{-1}x^{-1} = e$.

3. Unicità del reciproco: se y è un reciproco di x, si ha $y = ye = yxx^{-1} = ex^{-1} = x^{-1}$.

4. Unicità di e : se e ha la stessa proprietà di e si ha $e' = e'e = e$.

5. Proprietà $(x^{-1})^{-1} = x$: infatti da $xx^{-1} = e$ moltiplicando a destra per $(x^{-1})^{-1}$

   $xx^{-1}(x^{-1})^{-1} = e(x^{-1})^{-1}$ ovvero $x = (x^{-1})^{-1}$.

6. Proprietà $(xy)^{-1} = y^{-1}x^{-1}$:

   $(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}ey = y^{-1}y = e$.

Il Lemma 1 mostra che la definizione di gruppo che a priori sembra mostrare una "pericolosa" preferenza per la sinistra, è in realtà simmetrica, bipartisan, e avrebbe potuto essere data usando la destra.

Definizione 2. *Un gruppo G tale che per ogni x, $y \in G$*

$$xy = yx$$

si dice **commutativo** *o* **abeliano.**

Se G è un gruppo commutativo spesso si indica la legge di composizione con $+$ e si scrive $x + y$ al posto di xy, e la chiameremo quindi *addizione*, mentre l'elemento $x + y$ si chiama **somma**. In tal caso il gruppo si chiamerà *additivo* (l'essere additivo è una proprietà del gruppo non delle notazioni).
L'identità di un gruppo additivo G si indica di solito con 0 (**zero**) o $)_G$; scriveremo $-x$ (e si chiama **opposto** di x) in luogo di x^{-1}. Si scrive $x - y$ invece di xy^{-1}. Per un gruppo moltiplicativo l'identità si indica invece con 1 o 1_G.

Esempi

Esempio 1. Le matrici reali $m \times n$ formano un gruppo commutativo rispetto alla addizione. Siano

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}$$

Definiamo l'addizione $A + B$ nel modo che segue:

$$A + B = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \cdots & a_{2n} + b_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \cdots & a_{mn} + b_{mn} \end{pmatrix}$$

Esempio 2. I numeri complessi di modulo 1 formano un gruppo commutativo rispetto alla moltiplicazione.

Esempio 3. Le radici complesse del polinomio $P_n(z) = z^n - 1$ sono un gruppo commutativo rispetto alla moltiplicazione.

Esempio 4. Le matrici $n \times n$ (e, ad esempio reali), invertibili, formano un gruppo (*non commutativo*) per la moltiplicazione. Ovvero, se $A = \{a_{ij}\}_{i,j=1,\cdots n}$ e $B = \{b_{ij}\}_{i,j=1,\cdots,n}$, allora la matrice prodotto $C = AB$ ha la componente ik data da

$$c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}.$$

2 I numeri interi

Consideriamo sull'insieme $\mathbb{N}\times\mathbb{N}$ delle coppie (n, m) dei numeri naturali la seguente relazione di equivalenza:([1])

$$(n, m) \cong (n', m') \iff n + m' = n' + m$$

Sia $[n, m]$ la classe di equivalenza di (n, m), e sia I l'insieme delle classi, ovvero (vedi Capitolo 2) $I = \mathbb{N}\times\mathbb{N}/\cong$ e sia $P : (n, m) \longrightarrow [n, m]$ l'applicazione canonica di $\mathbb{N} \times \mathbb{N} \longrightarrow I$.
Definiamo:

$$[n, m] + [n', m'] = [n + n', m + m']. \tag{1}$$

Dimostriamo intanto che questa è una **buona definizione**, ossia che $[n, m] + [n' + m']$ dipende solo da $[n, m]$ ed $[n', m']$, e non per esempio da (n, m) : infatti se $[n, m] = [p, q]$, ossia se $(n, m) \cong (p, q)$ si ha
$(p + n', q + m') \cong (n + n', m + m')$ in quanto $p + n' + m + m' = n + n' + q + m'$; questo perché $p + m = n + q$.

Teorema 1. *L'insieme I sopra definito, con la legge di composizione $+$ è un gruppo commutativo additivo.*

Dim. Intanto, per ogni $a, b \in I$, segue da (1) che $a + b \in I$; controlliamo che siano verificate le tre proprietà che definiscono un gruppo, inoltre si deve controllare anche la commutatività.

Associatività: per definizione si ha:

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

Identità sinistra: l'identità sinistra è $[0, 0]$ perché $[0, 0] + [n, m] = [n, m]$.

Reciproco sinistro: dato $[n, m]$ dimostriamo che un suo reciproco sinistro è dato da $[m, n]$:

$[m, n] + [n, m] = [m + n, m + n] = [0, 0]$

Commutatvità: $[n, m] + [p, q] = [n + p, m + q] = [p, q] + [n, m]$.

Il gruppo I determinato dalla (1) si chiama **gruppo additivo degli interi**, e i suoi elementi si chiamano **numeri interi** o gli **interi** e si indicano con il simbolo $\mathbb{Z}$. In I possiamo definire un'altra legge di composizione detta **moltiplicazione** (e il suo risultato sarà detto **prodotto**) nel modo seguente:

Definizione 3.

$$[n, m][n'm'] = [nn' + mm', nm' + mn'].$$

Anche questa è una buona definizione: infatti, se $(n, m) \cong (p, q)$ si ha
$(nn' + mm', nm' + mn') \cong (pn' + qm', pm' + qn')$
in quanto
$nn' + mm' + pm' + qn' = pn' + qm' + nm' + mn'$, essendo $n + q = p + m$.

[1] Ricordiamo che su $\mathbb{N}$ "l'operazione somma" $n + m$ è stata definita nel capitolo precedente come la cardinalità dell'insieme costituito dall'unione di due insiemi disgiunti aventi ciscuno, rispettivamente, cardinalità n ed m.

Teorema 2. *Con la Definizione 3, per a, b, $c \in I$ si ha*
associatività del prodotto: $(ab)c = a(bc)$;
commutatività del prodotto: $ab = ba$;
identità per il prodotto: $[1,0]a = a$;
distributività del prodotto rispetto alla somma: $a(b+c) = ab + ac$ *(ossia* $= (ab) + (ac)$*);*
$(-a)b = -(ab) = -ab$;
legge di annullamento del prodotto: $ab = 0$ *se e solo se o* $a = 0$*, o* $b = 0$ *(o ambedue).*

Dim. Tutte le dimostrazioni si ottengono come applicazioni immediate delle definizioni. Vediamo qualche esempio.
Distributività: siano $a = [a_1, a_2]$, $b = [b_1, b_2]$, $c = [c_1, c_2]$; allora

$$\begin{aligned} a(b+c) = [a_1,a_2][b_1+c_1, b_2+c_2] &= [a_1b_1 + a_1c_1 + a_2b_2 + a_2c_2, a_1b_2 + a_1c_2 + a_2b_1 + a_2c_1] = \\ &= [a_1b_1 + a_2b_2, a_1b_2 + a_2b_1] + [a_1c_1 + a_2c_2, a_1c_2 + a_2c_1] = \\ &= [a_1,a_2][b_1,b_2] + [a_1,a_2][c_1,c_2] = ab + ac. \end{aligned}$$

legge di annullamento del prodotto: siano $a = [a_1, a_2]$, $b = [b_1, b_2]$, risulta
$ab = [a_1b_1 + a_2b_2, a_1b_2 + a_2b_1] = 0 = [0,0]$
se e solo se $a_1b_1 + a_2b_2 = a_1b_2 + a_2b_1$; questo accade intanto se $a = 0$ (ossia $a_1 = a_2$) oppure $b = 0$ (ossia $b_1 = b_2$); non accade però in altri casi, in quanto se, ad esempio, $a_1 < a_2$ la precedente si scrive $b_2(a_2 - a_1) = b_1(a_2 - a_1)$, donde $b_2 = b_1$, per le proprietà dei numeri naturali.([2])

Definizione 4. *Per a, $b \in I$, definiamo la corrispondenza $a < b$ nel modo seguente, posto $a = [a_1, a_2]$ e $b = [b_1, b_2]$:*

$$a < b \iff a_1 + b_2 < b_1 + a_2.$$

Questa é una buona definizione come si vede dal seguente teorema.

Teorema 3. *La corrispondenza (4) definita in $I \times I$ è un ordinamento totale di I; esso ha le proprietà seguenti:*

1. *se $a < b$, allora $a + c < b + c$;*
2. *se $a < b$ e $c > 0$, allora $ac < bc$;*
3. *$a < 0$ se e solo se $-a > 0$.*

Dim. Anche qui basta applicare in ogni caso le definizioni; diamo un esempio nel dimostrare che $<$ è un ordinamento totale; dati $a = [a_1, a_2]$ e $b = [b_1, b_2]$, vale una ed una sola tra le $a_1 + b_2 < b_1 + a_2$, $a_1 + b_2 = b_1 + a_2$, $a_1 + b_2 > b_1 + a_2$, ossia fra le $a < b$, $a = b$, $a > b$.
Se poi $c = [c_1, c_2]$, ed $a < b$, $b < c$, si ha $a_1 + b_2 < b_1 + a_2$, $b_1 + c_2 < c_1 + b_2$, donde, sommando $a_1 + b_1 + b_2 + c_2 < b_1 + b_2 + c_1 + a_2$ e perciò $a_1 + c_2 < c_1 + a_2$, ossia $a < c$.

Teorema 4. *L'applicazione di $\mathbb{N}$ su I definita da $n \longrightarrow [n,0]$ è una similititudine, e conserva le operazioni di addizione moltiplicazione. In altre parole, $n + m \longrightarrow [n,0] + [m,0]$, ed $nm \longrightarrow [n,0][m,0]$. Inoltre se $n \in \mathbb{N}$ $(n \geq 1)$ e $[h,k] \in I$ si ha*

$$n[h,k] = [n,0][h,k] = \overbrace{[h,k] + [h,k] + \cdots + [h,k]}^{n\text{ − volte}}$$

[2]Se $m, n, p \in \mathbb{N}$ e $mp = np$ allora $m = n$. Infatti, siano A,B, C tali che $card\, A = m$, $card\, B = n$, $card\, C = p$, quindi $card\,(A \times C) = mp$ e $card(B \times C) = np$. Non può essere $m < n$ perché altrimenti si avrebbe che esisterebbe una bigezione ψ di A in un sottoinsieme di B da cui seguirebbe che $\Psi : A \times C \longrightarrow B \times C$ definita da $\Psi(a,c) = (\psi(a), c)$ sarebbe una bigezione di $A \times C$ in un sottoinsieme di $B \times C$ e quindi $card(A \times C) < card(B \times C)$. Assurdo perché $mp = np$. Analogo discorso per verficare che non può essere $mp > np$.

Dim. Se $n < m$, per definizione è anche $[n,0] < [m,0]$; quindi l'applicazione è una similitudine. Il resto è immediato.

Per il Teorema 4 vi è una corrispondenza biunivoca tra tutto $\mathbb{N}$ e l'insieme dei numeri interi ≥ 0; ed elementi corrispondenti si comporteranno allo stesso modo rispetto alla somma, al prodotto, ed all'ordinamento. Possiamo quindi indicare l'elemento $[m,0]$ con m; in tal modo l'intero $[n,m] = [n,0] - [m,0]$ sarà indicato con $n - m$; l'insieme degli interi diviene allora l'unione di $\mathbb{N}$, e degli interi < 0 che sono anche quelli della forma $-n$, con $n > 0$ (vedi Teorema 3); gli interi > 0 (< 0) si dicono **positivi** (**negativi**). I positivi e lo zero restano quindi identificati con i naturali.

Definizione 5. *Sia G un gruppo, g un suo elemento, n intero; la* **potenza** *$n-$esima di g, scritta g^n è così definita:*

$$\begin{array}{lcl} g^0 & = & 1_G; \\ g^n & = & \overbrace{g\, g \cdot \cdots \cdot g}^{n \text{ volte}}; \\ g^{-n} & = & (g^{-1})^n \quad \text{se } n > 0. \end{array}$$

*Il numero n dicesi l'***esponente**

Teorema 5. *Sia G un gruppo, e siano g, h suoi elementi tali che $gh = hg$. Siano n, m interi; allora:*

$$g^{n+m} = g^n g^m, \quad g^{nm} = (g^n)^m, \quad (gh)^n = g^n h^m.$$

Dim. Dimostriamo come esempio la prima relazione:
se m, n sono intri essa è una conseguenza immediata della definizione; stesso discorso se uno di essi è nullo. Sia $n < 0$, e $-n < m$; allora

$$\begin{array}{rcl} g^n g^m & = & (g^{-1})^{-n} g^m = \underbrace{g^{-1} \cdots g^{-1}}_{-n} \ \underbrace{g \cdots g}_{m} = \\ & = & \underbrace{g^{-1} \cdots g^{-1}}_{-n-1} \ \underbrace{g \cdots g}_{m-1} = \\ & = & \cdots = g^{-1} \ \underbrace{g \cdots g}_{m+n+1} = \underbrace{g \cdots g}_{m+n} = g^{m+n}. \end{array}$$

Sia infine $n < 0$, ed m qualsiasi; sia q intero abbastanza grande; allora, per quanto visto sopra,
$g^{n+m+q} = g^{n+m} g^q$, ed anche
$g^{n+m+q} = g^n g^{m+q} = g^n g^m g^q$.
Pertanto
$g^{n+m} g^q = g^n g^m g^q$, donde, moltiplicando a destra per $(g^q)^{-1}$ si ricava $g^{n+m} = g^n g^m$.

3 Sottogruppi

Definizione 6. *Un sottoinsieme H del gruppo G è un* **sottogruppo** *di G (e G è un* **sopragruppo** *di H) se è un gruppo rispetto alla legge di composizione in G. Se H è già dato con una sua legge di composizione, occorrerà anche che tale legge coincida, in H, con quella di G.*

Lemma 2. *Un sottoinsieme non vuoto H del gruppo G è un sottogruppo di G se e solo se $g\, h^{-1} \in H$ per ogni $g, h \in H$.*

Dim. Se H è un sottogruppo ovviamente la condizione è verificata. Viceversa supponiamo verificata la la condizione, allora H contiene l'identità $1 = 1_g = 1_H$, in quanto contiene $gg^{-1} = 1$ per $g \in H$; poi se $g \in H$ anche $g^{-1} \in H$, in quanto $g^{-1} = 1g^{-1}$; infine se $g, h \in H$, si ha $gh = g(h^{-1})^{-1} \in H$. Non occorre verificare l'associatività e perciò l'asserto è provato.

Definizione 7. *Siano G e K gruppi, e sia σ un'applicazione di G su K; σ è un* **omomorfismo** *se*

$$\sigma(gg') = (\sigma\, g)(\sigma\, g'), \quad \forall g, g' \in G.$$

Inoltre
isomorfismo *è un omomorfismo biunivoco;*
endomorfismo *è un omomorfismo di un gruppo su se stesso;*
automorfismo *è un isomorfismo di un gruppo su se stesso.*
Due gruppi G, K sono isomorfi se esiste un isomorfismo di G su tutto K, (in tal caso ve n'è uno di K su tutto G)

Sia σ un omomorfismo del gruppo G sul gruppo K; osserviamo che

$$\sigma\, 1_G \,=\, 1_K, \quad \text{in quanto} \quad (\sigma\, 1_G)(\sigma\, 1_G) \,=\, \sigma\,(1_G\, 1_G) \,=\, \sigma\, 1_G.$$

Chiameremo **nucleo**([3]) di σ l'insieme:

$$\ker \sigma \,=\, \{g :\ g \in G \text{ tali che } \quad \sigma g = 1_K\}$$

Si verifica che $\ker \sigma$ è un sottogruppo di G. Infatti osserviamo che, per ogni g, $h \in H$ si ha:
$1_K = \sigma(g) = \sigma(gh^{-1}h) = \sigma(gh^{-1})\sigma(h) = \sigma(gh^{-1})\, 1_K = \sigma(gh^{-1})$. Dal Lemma 2 si ha la tesi.

Teorema 6. *Un omomorfismo è un isomorfismo se e solo se il suo nucleo è $\{1\}$.*

Dim.
Siano G, K due gruppi e $\sigma : G \longrightarrow K$ un omomorfismo. Supponiamo che sia un isomorfismo. Se esistesse $g \in \ker \sigma$ con $g \neq 1_G$ si avrebbe l'assurdo perché

$$\sigma g = \sigma 1_G,$$

e quindi σ non sarebbe iniettiva.
Viceversa supponiamo che $\ker \sigma = \{1_G\}$, allora da $\sigma g = \sigma g'$ moltiplicando per $\sigma g'^{-1}$ otteniamo

$$\sigma g(\sigma g'^{-1}) = \sigma g'(\sigma g'^{-1}) = \sigma(g' g'^{-1}) == \sigma 1_G = 1_K \iff \sigma(g\, g'^{-1}) = 1_K \iff g\, g'^{-1} = 1_G \iff g = g'$$

4 I gruppi ordinati e i razionali

Sia G è un gruppo additivo. Ricordiamo che se $g \in G$ e $n \in \mathbb{N}$, $n > 0$ con l'espressione ng significa $\overbrace{g + g + \cdots + g}^{n \text{ volte}}$.

Definizione 8. *Un gruppo additivo G si dice* **divisibile** *se per ogni $g \in G$ ed ogni intero $n > 0$ esiste almeno un $h \in G$ tale che $nh = g$*

Definizione 9. Un gruppo ordinato *è una terna $(\Gamma, +, <)$, dove $(\Gamma, +)$ è un gruppo (commutativo) additivo, e $(\Gamma, <)$ è un insieme ordinato, soddisfacente la relazione $\alpha + \gamma < \beta + \gamma$ ogniqualvolta $\alpha < \beta$ (ove α, β, $\gamma \in \Gamma$). Diremo che Γ è un gruppo ordinato e sottointenderemo $+$ e $<$; esso può anche essere scritto come gruppo moltiplicativo. L'insieme dei $\Gamma > 0$ si indica con Γ^+, e i suoi elementi si dicono* **positivi***; quello dei $\gamma < 0$ si indica con Γ^- e i suoi elementi si dicono* **negativi**.

[3] In inglese **kernel**.

Esempi

Esempio 1. Il gruppo additivo degli interi, ordinato mediante $<$ è un gruppo ordinato e non è divisibile.

Esempio 2. Il gruppo additivo dei razionali, ordinato mediante $<$, è un gruppo ordinato ed è divisibile.

Esempio 3. Il gruppo moltiplicativo delle radici $n-esime$ complesse dell'unità non è ordinabile (in modo da diventare un gruppo ordinato) e non è divisibile.

Esempio 4. Il gruppo di tutte le radici $n-$esime dell'unità non è ordinabile ed è divisibile.

Teorema 7. *Sia Γ un gruppo ordinato; allora esistono sopragruppi ordinati divisibili Γ' di Γ (il cui ordinamento induca in Γ l'ordinamento dato). Fra questi vi è Δ con la proprietà seguente:*

$$\forall \delta \in \Delta \ \ \exists n \ \text{ tale che } \ n\,\delta \in \Gamma.$$

Tale Δ è unico e minimo nel senso seguente:
se Γ' è come detto al principio, esiste un isomorfismo di Δ su Γ' che è anche una similitudine, e che induce l'isomorfismo identico di Γ su Γ.

Dim. Sia S l'insieme delle coppie (α, n), con $\alpha \in \Gamma$ ed n intero positivo; definiamo in S la relazione di equivalenza $\cong$ nel modo seguente

$$(\alpha, n) \cong (\beta, m) \iff m\,\alpha = n\,\beta;$$

sia $[\alpha,\ n]$ la classe contenente $(\alpha,\ n)$ ossia l'immagine della proiezione di S sull'insieme quoziente Δ di S modulo $\cong$ ovvero $\Delta = S/\cong$. Δ diviene un gruppo additivo mediante la definizione seguente:

$$[\alpha, n] + [\beta, m] = [m\alpha + n\beta, mn];$$

non è difficile verificare che questa è una buona definizione e che rende Δ un gruppo. Ordiniamo Δ col porre

$$[\alpha, n] < [\beta, m] \iff m\alpha < n\beta$$

si verifica che questa è una buona definizione e che $<$ è un ordinamento totale. Allora Δ è un gruppo ordinato, perchè se
$[\alpha, n] < [\beta, m]$ è anche $[\alpha, n] + [\gamma, q] < [\beta, m] + [\gamma, q]$.
Il gruppo Δ è divisibile: dati infatti $[\alpha, n] \in \Delta$, e l'intero positivo m, si ha $m[\alpha, mn] = [\alpha, n]$
Infine, Δ contiene un sottogruppo isomorfo e simile a Γ : il sottogruppo formato dagli $[\alpha, 1]$. Se si identifica Γ con tale sottogruppo, Δ diviene uno dei Γ' di cui il teorema asserisce l'esistenza.
Sia Γ' un qualsiasi sopragruppo ordinato divisibile di Γ; l'isomorfismo σ di Δ su Γ' si definisce così:
dato $[\alpha, n] \in \Delta$, si cerchi un $\gamma' \in \Gamma'$ tale che $n\gamma' = \alpha$; tale γ' esiste perché Γ' è divisibile; poi è unico, perché da $n\gamma'' = \alpha$ segue $n(\gamma'' - \gamma') = 0$, onde $\gamma'' = \gamma'$.([4]) Si porrà allora: $\sigma[\alpha, n] = \gamma'$.

Il Δ costruito sopra si chiama il *minimo sopragruppo divisibile* di Γ. Il suo elemento $[\alpha, n]$ sarà indicato con α/n o con $n^{-1}\alpha$. Se in particolare Γ è il gruppo additivo degli interi il relativo Δ si chiama il **gruppo additivo (ordinato) dei (numeri) razionali**, e si indica con $\mathbb{Q}$. Nei paragrafi pracedenti abbiamo anche visto che tra i numeri interi è anche definibile l'operazione prodotto; tale operazione è estendibile ai numeri razionali ponendo

$$(n^{-1}m)(r^{-1}s) = (nr)^{-1}(ms)$$

Si verifica facilmente che tutte le asserzioni fatte per i numeri interi nei Teoremi 2 e 3 valgono per i numeri razionali.

[4] Segue dal fatto che se $n(\gamma' - \gamma'') = 0$ allora $\gamma' = \gamma''$. Infatti, supponiamo per assurdo che: $\gamma' < \gamma''$, da questo, procedendo per induzione, se $(n-1)\gamma' < (n-1)\gamma''$ allora, essendo Γ' un gruppo ordinato,
$n\gamma' = (n-1)\gamma' + \gamma' < (n-1)\gamma'' + \gamma' < (n-1)\gamma'' + \gamma'' = n\gamma''$. Discorso analogo se fosse $\gamma' > \gamma''$.

Sia Γ un gruppo ordinato, e sia $r = n^{-1}m$ un numero razionale; per $\alpha \in \Gamma$, indicheremo con $r\alpha$ l'elemento $n^{-1}(m\alpha) = m(n^{-1}\alpha)$ del minimo sopragruppo divisibile di Γ; valgono le proprietà.

$(r+s)\alpha = r\alpha + s\alpha$;
$r(\alpha+\beta) = r\alpha + r\beta$;
$r\alpha < s\alpha$ se $r < s$ ed $\alpha > 0$;
$r\alpha < r\beta$ se $\alpha < \beta$ ed $r > 0$;
$r\alpha = 0$ se e solo se o $r = 0$, o $\alpha = 0$;
$(rs)\alpha = r(s\alpha)$;
$r(-\alpha) = (-r)\alpha = -(r\alpha)$.

5 I gruppi archimedei e i numeri reali

Definizione 10. *Un sottogruppo ordinato Δ di un gruppo ordinato Γ dicesi* **isolato** *se Δ^+ è segmento di Λ^+.*

Il **rango** *di un gruppo ordinato è la cardinalità, diminuita di uno se finita, dell'insieme dei sottogruppi isolati; il solo gruppo di rango zero è quello banale; i gruppi di rango 1 si dicono* **archimedei.**

Lemma 3. *Sia Γ un gruppo ordinato, e ne sia Δ il minimo sopragruppo divisibile. Allora Γ e Δ hanno lo stesso rango.*

Dim.
Per ogni sottogruppo isolato Δ' di Δ, il $\Gamma' = \Delta' \cap \Gamma$ è sottogruppo isolato di Γ; se $\Delta' \subset \Delta''$, è certo $\Gamma' \subset \Gamma''$, in quanto scelto un δ di Δ'', ma non di Δ', per un opportuno intero positivo n l'elemento $n\delta$ appartiene a Γ'' ma non a Γ' (se appartenesse a Γ', apparterrebbe anche a Δ', impossibile perché se, per es. $\delta > 0$, è anche $n\delta > \delta$, e δ è maggiore di ogni elemento di Δ' in quanto Δ' è isolato). Pertanto l'applicazione $\Delta' \longrightarrow \Gamma'$ è un'applicaizone biunivoca dell'insieme dei sottogruppi isolati di Δ su quello dei sottogruppi isolati di Γ. È poi su tutto tale insieme: se Γ' è sottogruppo isolato di Γ, l'insieme degli $r\gamma$, con r numero razionale e $\gamma \in \Gamma'$, è un sottogruppo isolato Δ' di Δ, tale che $\Delta' \cap \Gamma = \Gamma'$.

Teorema 8. *Un gruppo ordinato non banale Γ è archimedeo se e solo se soddisfa al seguente* **"postulato di Archimede"***:*
se α, $\beta \in \Gamma^+$, esiste un intero positivo n tale che $n\alpha > \beta$.

Dim.
Sia Γ archimedeo, e sia $0 < \alpha < \beta \in \Gamma$; sia Δ l'insiem di tutti i $\gamma \in \Gamma$ per ciascuno dei quali esiste un intero n tale che $-n\alpha < \gamma < n\alpha$. Allora Δ è un sottogruppo isolato di Γ, contenente $\alpha \neq 0$. quindi $\Delta = \Gamma$, $\beta \in \Delta$, e $\beta < n\alpha$ per qualche intero n.

Reciprocamente, si supponga che Γ soddisfi al postulato di Archimede, e ne sia $\Delta \neq \{0\}$ un sottogruppo isolato. Se $\alpha \in \Delta^+$ e $\beta \in \Gamma^+$, per un opportuno intero positivo n si ha $\beta < n\alpha$, onde $\beta \in \Delta$; perciò $\Delta = \Gamma$, e Γ è archimedeo.

Definizione 11. *Un gruppo archimedeo Γ è discreto se Γ^+ ha un elemento minimo(ossia un primo elemento).*

Teorema 9. *Un gruppo ordinato è archimedeo discreto se e solo se è isomorfo e simile al gruppo ordinato degli interi.*

Dim. Sia Γ archimedeo discreto, e sia e il minimo di Γ^+; sia $\mathbb{Z}$ il gruppo additivo degli interi, e si definisca l'applicazione σ di $\mathbb{Z}$ su Γ nel modo seguente: $\sigma n = ne$; σ é ovviamente un isomorfismo ordinato; è poi su tutto Γ perché ogni elemento di Γ è della forma ne : dato $\alpha \in \Gamma^+$, non può essere $ne < \alpha$ per ogni $n \in \mathbb{Z}$; detto n il minimoper cui $ne \geq \alpha$, non può neppure essere $ne > \alpha$, in quanto da $(n-1)e < \alpha < ne$ seguirebbe $0 < \alpha - (n-1)e < e$, contro la ipotesi che e sia il minimo di Γ^+.

Lemma 4. *Un gruppo archimedeo è non discreto se e solo se, come insieme ordinato, è denso in sè.*

Dim.
Se Γ è denso in sè, per ogni $\alpha \in \Gamma^+$ vi è un certo elemento di Γ fra 0 ed α, onde Γ^+ non ha minimo. Reciprocamente, sia Γ non discreto, e siano α, $\beta \in \Gamma$, con $\alpha < \beta$; sia $0 < \gamma < \beta - \alpha$; allora $\alpha < \alpha + \gamma < \beta$, onde Γ è denso in sè.

Teorema 10. *Sia Γ un gruppo archimedeo non discreto, e sia Δ il completamento dell'insieme ordinato Γ. Vi è un sol modo di definire in Δ una legge di composizione che renda Δ un sopragruppo ordianto di Γ. Ed allora Δ è archimedeo non discreto.*

Dim. Intanto il completamento Δ di Γ esiste per il Teorema sul completamento degli insiemi ordinati (vedi Capitolo terzo) , in quanto Γ è privo di minimo, di massimo, e anche di salti per il Lemma 4 ed il Lemma sugli insiemi densi in sè del Capitolo terzo.

Ogni $\delta \in \Delta$ definisce un segmento $S_\delta = \{\alpha : \alpha \in \Gamma, \alpha < \delta\}$ di Γ; dati γ, $\delta \in \Delta$, l'insieme $S_\gamma + S_\delta = \{\alpha + \beta : \alpha \in S_\gamma, \beta \in S_\delta\}$ è un non vuoto, ed è dotato di maggioranti (per esempio $\alpha' + \beta'$ se $\alpha' \notin S_\gamma$ e $\beta' \notin S_\delta$); pertanto per il Teorema sugli estremi superiori di insiemi ordinati (vedi Capitolo terzo): $S_\gamma + S_\delta$ ha in Δ, l'estremo superiore; tale elemento sarà indicato con $\gamma + \delta$; si noti subito che $S_\gamma + S_\delta$ è un segmento, che coincide quindi con $S_{\gamma+\delta}$. Prima di dimostrare che questa definizione rende Δ un sopragruppo ordinato di Γ, dimostriamo che è l'unica definizione che può raggiungere tale scopo. Se infatti Δ è con un'operazione $\oplus$, sopragruppo ordinato di Γ, dall'essere γ, δ maggioranti di S_γ, S_δ segue intanto che $\gamma \oplus \delta$ deve essere maggiorante di $S_\gamma \oplus S_\delta = S_\gamma + S_\delta$. D'altra parte se γ', δ' sono maggioranti in Γ di S_γ, S_δ rispettivamente, si avrà $\gamma' \geq \gamma$, $\delta' \geq \delta$, onde $\gamma' + \delta' = \gamma' \oplus \delta' \geq \gamma \oplus \delta$; siccome ogni maggiorante in Γ di $S_\gamma + S_\delta$ è della forma $\gamma' + \delta'$, si conclude $\gamma \oplus \delta$ è il minimo maggiorante (in Δ) di $S_\gamma + S_\delta$, ossia ne è l'estremo superiore; ma ciò significa appunto che $\gamma \oplus \delta = \gamma + \delta$.

Resta da dimostrare che con la legge + il Δ è effettivamente un sopragruppo ordinato di Γ; intanto induce in Γ la legge già esistente, come si vede in modo analogo alla precente dimostrazione di unicità; poi:

1. Associatività: $(\gamma+\delta)+\varepsilon$ è l'estremo superiore di $S_{\gamma+\delta}+S_\varepsilon = S_\gamma+S_\delta+S_\varepsilon$; e lo stesso vale per $\gamma+(\delta+\varepsilon)$.
2. Commutatività: ovvia.
3. Esistenza dello 0 : è $\delta + 0 = \delta$ perché $S_{\delta+}S_0 = S_\delta$.
4. Esistenza del reciproco (opposto): se $\delta \in \Delta$, $-\delta$ è l'estremo superiore del segmento $\{-\alpha : \alpha \in \Gamma, \alpha > \delta\}$.
5. Δ è un gruppo ordinato: se $\delta < \gamma$, e se $\varepsilon \in \Delta$, si ha $\delta + \varepsilon < \gamma + \varepsilon$ perché $S_\delta + S_\varepsilon \subset S_\gamma + S_\varepsilon$.

Resta infine da vedere che Δ è archimedeo non discreto; se γ, $\delta \in \Delta^+$ si scelgano α, $\beta \in \Gamma^+$ tali che $\alpha < \gamma$, $\beta > \delta$; per il Teorema 8, esiste un intero positivo n tale che $n\alpha > \beta$; ma allora $n\gamma > \delta$, il che prova che Δ è archimedeo. Esso è poi ovviamente non discreto.

Il gruppo ordinato Δ di cui il precedente Teorema asserisce l'esitenza viene chiamato il **completamento** di Γ (come gruppo ordinato).

Teorema 11. *Un gruppo ordinato archimedeo è completo come insieme ordinato se e solo se non è sottogruppo ordinato proprio di nessun gruppo ordinato archimedeo.*

Dim.
Se Γ non è completo, si possono presentare due casi:
1. Γ ha salti; in tal caso Γ è discreto per il Lemma 4 e per il Lemma sugli insiemi densi in sè del Capitolo terzo,ed allora non è divisibile, ed ha un sopra gruppo proprio archimedeo, per il Teorema 7 e il Lemma 3.

2. Γ non ha salti, nel qual caso è denso in sè sempre per per il lemma sugli insiemi densiin sè del Capitolo terzo, ed è non discreto per il Lemma 4. Ha allora un completamento archimedo Γ', per il Teorema 10, e si ha $\Gamma' \supset \Gamma$ perché Γ' è completo e Γ non lo è; questa è appunto la tesi.

Reciprocamente, sia Γ sottogruppo ordinato prorpio di un Δ archimedo; sarà anche un sottogruppo proprio del completamento di Δ, onde si può supporre che Δ sia completo; occorre dimostrare che Γ non è completo.

Se Γ è discreto, ciò è certamente vero; se Γ è non discreto, la dimostrazione procede così:

1. Per ogni n intero positivo, ed ogni $\gamma \in \Gamma^+$, esite un $\gamma_n \in \Gamma^+$ tale che $2^n\,\gamma_n < \gamma$: infatti, per $n = 1$ basta prendere un γ'' fra 0 e γ, e scegliere un $\gamma_1 \in \Gamma^+$ che sia minore di γ'' e di $\gamma - \gamma''$, per avere $2\gamma_1 < \gamma$; se poi si trova γ_2 in modo che $2\gamma_2 < \gamma_1$, sarà $2^2\,\gamma_2 < \gamma$, e così via.
2. Γ è denso in Δ : dati $0 < \delta < \delta' \in \Delta$, e dato $\gamma \in \Gamma^+$, nelle notazioni del punto precedente è certamente $\gamma_n < \delta' - \delta$ per qualche n : altrimenti $2^n(\delta' - \delta) < \gamma$ per ogni n in contraddizione con il Teorema 8. Ed allora se m è il minimo inteero tale che $m\gamma_n > \delta$, si ha $\delta < m\gamma_n < \delta'$, come voluto.
3. Dal punto precedente segue che Δ è il completamento di Γ; dall'essere $\Gamma \subset \Delta$, e dal Teorema sui completamenti degli insiemi ordinati, visto nel Capitolo terzo, segue allora che Γ non era completo.

Corollario 1. *Un gruppo archimedeo completo è divisibile.*

Dim. Discende dai Teoremi 11 e 7, e dal Lemma 3.

Il completamento del gruppo additivo dei razionali è chiamato il gruppo ordinato (additivo) dei **numeri reali** e si indica con $\mathbb{R}$.