Chapter 1

RICHIAMI DI ARITMETICA

1.1 INTERI RELATIVI E DIVISIBILITA'

Proposizione 1.1.1 *Se* $a, b \in \mathbb{Z},\ b \neq 0$, *esistono unici* $q, r \in \mathbb{Z}$ *tali che risulti* $a = bq + r$, *con* $0 \leq r <\mid b \mid$; q *e* r *sono detti rispettivamente quoziente e resto della divisione di* a *per* b .

Dimostrazione - Nel caso $a = 0$ la tesi segue assumendo $q = r = 0$; sia quindi $a \neq 0$. Siano ora $b > 0$ e $S = \{n \in \mathbb{Z}/n = a - bt \geq 0,\ t \in \mathbb{Z}\}$; tale insieme è non vuoto in quanto $b \mid a \mid \geq \mid a \mid$, essendo $b \geq 1$, onde $n = a - b(- \mid a \mid) \geq 0$ e quindi $n \in$S.

Sia dunque $r = a - bq$ il minimo di S, esistente per il principio del minimo; dimostriamo che r è il resto della divisione di a per b. Ovviamente $0 \leq r$, poiché $r \in S$; se per assurdo fosse $b \leq r$ allora risulterebbe $0 \leq r' = r - b = = a - bq - b = a - b(q + 1)$, onde $r' \in S$ e $r' < r$, il che è assurdo essendo r il minimo di S. Esaminiamo ora il caso $b < 0$; possiamo allora dividere a per $-b$ ottenendo $a = (-b)q' + r'$, $0 \leq r' < -b$, onde $a = b(-q') + r'$, $0 \leq r' <\mid b \mid$, e pertanto il quoziente e il resto della divisione di a per b sono rispettivamente $-q'$ e r'.

Per quanto riguarda l'unicità di q e r, sia $a = bq + r = bq' + r'$, con $0 \leq r <\mid b \mid$, $0 \leq r' <\mid b \mid$; supposto $r \leq r'$, si ha $r' - r = b(q - q')$ ed essendo $0 \leq r' - r <\mid b \mid$ segue quindi che $r' = r$ e $q = q'$. ∎

Definizione 1.1.1 Si dice che l'intero b *divide* l'intero a se esiste un intero c tale che risulti $a = b \cdot c$.

Equivalentemente potremmo dire che b divide a se, nella divisione con resto di a per b, il resto è nullo.

Definizione 1.1.2 Se $a, b \in \mathbb{Z}\backslash\{0\}$ si definisce *massimo comun divisore fra a e b*, e si denota (a, b), un intero $d \in \mathbb{Z}$ tale che:
i) $a = ds$, $b = dt$, $s, t \in \mathbb{Z}$;
ii) $c \in \mathbb{Z}$ / $a = cs'$, $b = ct' \Rightarrow d = ck$, $k \in \mathbb{Z}$.

L'esistenza di un intero che goda di tali proprietà è assicurata dalla proposizione che segue.

Proposizione 1.1.2 *Se $a, b \in \mathbb{Z}\backslash\{0\}$, allora il massimo comun divisore fra a e b esiste ed è unico a meno del segno.*

Dimostrazione - Sia $S = \{ax + by \ / \ x, y \in \mathbb{Z},\ ax + by > 0\}$; si ha allora che S è non vuoto poiché, prendendo x positivo o negativo a seconda che a sia positivo o negativo e, analogamente, prendendo y positivo o negativo a seconda che b sia positivo o negativo, il numero $ax + by$ risulterà essere positivo.

Per il principio del minimo in $\mathbb{N}$ esiste $d \in S$, $d = ah + bk$, minimo in S; dimostriamo che d è un massimo comun divisore di a e b. Dividendo a per d, si ottiene $a = dq + r$, $0 \leq r < d$; poiché $r = a - dq = a(1 - hq) + b(-kq)$, se fosse $0 < r$ risulterebbe $r \in S$ contro la minimalità di d. Pertanto $r = 0$ onde $a = dq$; in modo analogo si dimostra che $b = dq'$. Se poi $c \in \mathbb{Z}$ è tale che $a = cs'$ e $b = ct'$, allora $d = ah + bk = cs'h + ct'k = c(s'h + t'k)$, onde la ii) della definizione 1 è verificata.

Infine, per quanto riguarda l'unicità del massimo comun divisore a meno del segno, sia d' un altro massimo comun divisore di a e b; ora, per la ii) applicata al massimo comun divisore d', si ha $d' = md$, mentre per la ii) applicata al massimo comun divisore d, risulta $d = nd'$, onde $d = nmd$ e quindi $d(1 - nm) = 0$. Da ciò segue che, essendo $d \neq 0$, $nm = 1$ e pertanto $n = m = \pm 1$. ∎

Osservazione 1.1.1 Dalla dimostrazione appena fatta segue che il massimo comun divisore d fra due interi non nulli a e b si può sempre scrivere nella forma $d = ah + bk$, $h, k \in \mathbb{Z}$; tale identità prende il nome di *identità di Bézout*. Inoltre il massimo comun divisore (a, b) divide ogni intero della forma $ax + by$, $\forall\ x, y \in \mathbb{Z}$.

Un utile metodo di calcolo del massimo comun divisore tra due interi utilizza la divisione euclidea; infatti si può dimostrare che:

Lemma 1.1.1 *Se $a, b \in \mathbb{Z}\backslash\{0\}$, $a = bq + r$, $0 \leq r <\mid b \mid$, allora $(a, b) = (b, r)$.*

Dimostrazione - Sia $d = (a, b)$, $a = ds$, $b = dt$; allora $r = a - bq = d(s - tq)$. Per dimostrare che $d = (b, r)$ resta quindi da dimostrare che, se $c \in \mathbb{Z}$ è tale che $b = cs'$ e $r = ct'$, allora d è un multiplo di c; risulta infatti $a = bq + r = c(s'q + t')$, onde, poiché c divide sia a che b e $d = (a, b)$, per la ii) della definizione 1.1.2, c divide d. ∎

Come conseguenza di questo lemma otteniamo un algoritmo molto semplice, l'algoritmo euclideo delle divisioni successive, per il calcolo del massimo comun divisore fra due interi non nulli e per la determinazione dei coefficienti dell'identità di Bézout.

Proposizione 1.1.3 (Algoritmo euclideo) *Il massimo comun divisore fra due interi non nulli a e b è l'ultimo resto non nullo della seguente serie di divisioni successive:*

$$\begin{array}{lcl} a & = & bq + r \\ b & = & rq_1 + r_1 \\ r & = & r_1q_2 + r_2 \\ r_1 & = & r_2q_3 + r_3 \\ \vdots & \vdots & \vdots \quad \vdots \quad \vdots \\ r_{n-2} & = & r_{n-1}q_n + r_n \\ r_{n-1} & = & r_nq_{n+1} \end{array}$$

ovvero $(a, b) = r_n$.

Dimostrazione - Per quanto dimostrato nel lemma 1.1.1 risulta:

$$(a, b) = (b, r) = (r, r_1) = \ldots = (r_{n-1}, r_n);$$

d'altra parte $r_{n-1} = r_nq_{n+1}$ e quindi $(r_{n-1}, r_n) = r_n$.

I coefficienti h e k dell'identità di Bézout possono essere calcolati al modo seguente: si esprime r_n in funzione di r_{n-2} e r_{n-1} , si esprime poi r_{n-1} in funzione di r_{n-2} e r_{n-3} e si sostituisce questa espressione nella precedente ottenendo r_n in funzione di r_{n-2} e r_{n-3}. Procedendo in tal modo si ottiene, alla fine, r_n in funzione di a e b. ∎

Esemplifichiamo ora il procedimento esposto nel teorema precedente.

Esempio 1.1.1 Se $a = 652$ e $b = 38$ risulta:

$$\begin{array}{rcl} 652 & = & 38 \cdot 17 + 6 \\ 38 & = & 6 \cdot 6 + 2 \\ 6 & = & 2 \cdot 3 \end{array}$$

e pertanto risulta (652,38)=2; inoltre:

$$2 = 38 + 6 \cdot (-6) \quad \text{e} \quad 6 = 652 + 38 \cdot (-17),$$

da cui $2 = 38 + [652 + 38 \cdot (-17)] \cdot (-6) = 652 \cdot (-6) + 38 \cdot 103$. Pertanto gli interi h e k dell'identità di Bézout sono, in questo caso, questo caso, $h = -6$ e $k = 103$.

Osservazione 1.1.2 Osserviamo che gli interi h e k? dell'identità di Bézout non sono unici. Si verifica infatti facilmente che $d = (a, b) = ah + bk = ah' + bk'$ se, e solo se, $h' = h + bt$ e $k' = k - at$, $\forall\, t \in \mathbb{Z}$; ad esempio nel caso precedente risulta anche $2 = 652 \cdot 32 + 38 \cdot (-549)$ (avendo considerato $t = 1$).

Osservazione 1.1.3 La nozione di massimo comun divisore può essere estesa a tre o più interi non nulli; infatti è facile verificare, e lo studente è invitato a farlo, che $((a, b), c) = (a, (b, c))$.

Definizione 1.1.3 Un intero p diverso da 0 e da ± 1 si dice *irriducibile* se, ogniqualvolta $p = a \cdot b$, risulta che $p = \pm a$ e $b = \pm 1$ oppure $p = \pm b$ e $a = \pm 1$

Definizione 1.1.4 Un intero p diverso da 0 e da ± 1 si dice *primo* se, ogniqualvolta p divide un prodotto $a \cdot b$, si ha che p divide uno dei due fattori; ovvero:

$$p|a \cdot b \quad \Rightarrow p|a \text{ oppure } p|b$$

Osservazione 1.1.4 La definizione di elemento primo è più forte di quella di elemento irriducibile nel senso che, se un elemento p è primo e risulta $p = a \cdot b$, allora p dividendo il prodotto $a \cdot b$ deve dividere uno dei due fattori. Risulta allora che $p|a$ oppure $p|b$; d'altra parte a e b dividono entrambi p e quindi $p = \pm a$ oppure $p = \pm b$, onde p è irriducibile.

Per i numeri interi vale inoltre la seguente proposizione.

Proposizione 1.1.4 *In $\mathbb{Z}$ un intero p risulta essere irriducibile se, e solo se, esso è primo.*

Dimostrazione - Avendo già osservato che ogni primo è irriducibile dimostriamo che, in $\mathbb{Z}$, ogni irriducibile è primo.

Sia dunque p un intero irriducibile e supponiamo che $p|a \cdot b$ ovvero $a \cdot b = p \cdot t$ per un opportuno $t \in \mathbb{Z}$; vogliamo dimostrare che p divide uno dei due fattori a e b. Supponiamo che p non divida a allora $(a, p) = 1 = ar + ps$ con r e s interi; moltiplicando l'identità di Bézout per b otteniamo:

$$b = abr + pbs = ptr + pbs = p(tr + bs)$$

e quindi p divide b, come volevamo dimostrare. ∎

A questo punto possiamo dimostrare un importante teorema.

Teorema 1.1.1 (Teorema fondamentale dell'aritmetica) *Ogni intero n diverso da 0 e da ± 1 si può fattorizzare al modo seguente:*

$$n = \pm p_1^{h_1} p_2^{h_2} \cdot \ldots \cdot p_t^{h_t}$$

dove i p_i sono primi positivi distinti e gli esponenti sono positivi. Tale rappresentazione inoltre risulta essere unica a meno dell'ordine dei fattori.

Dimostrazione - Dimostriamo innanzitutto, utilizzando il principio di induzione, che esiste una fattorizzazione del tipo richiesto per ogni intero positivo maggiore di uno e quindi, ovviamente, per ogni intero diverso da 0 e da ± 1.

Per $n = 2$, base dell'induzione, il teorema è vero essendo 2 un numero primo; supponiamo ora che il teorema sia vero per tutti i naturali m compresi fra 2 e n e dimostriamolo per n. Se n è un primo non c'è nulla da dimostrare, in caso contrario per quanto appena dimostrato n non è irriducibile e quindi esistono due interi a e b, $2 \leq a, b \leq n - 1$, tali che $n = a \cdot b$; per l'ipotesi induttiva i

due interi a e b possono essere fattorizzati in potenze di primi distinti e quindi anche n si può fattorizzare allo stesso modo.

Dobbiamo ora dimostrare che la fattorizzazione di un intero diverso da 0 e da ± 1 è unica a meno dell'ordine dei fattori; sia quindi:

$$n = \pm p_1^{h_1} p_2^{h_2} \cdot \ldots \cdot p_t^{h_t} = \pm q_1^{k_1} q_2^{k_2} \cdot \ldots \cdot q_s^{k_s}$$

con i q_j primi positivi distinti. Poiché il prodotto in $\mathbb{Z}$ è commutativo, possiamo ovviamente supporre che i primi delle due rappresentazioni siano ordinati in ordine crescente, dobbiamo allora dimostrare che $t = s$, $p_i = q_i$ e $h_i = k_i$, $\forall$ $i = 1, \ldots t$.

Dimostriamo anche questa parte per induzione sulla lunghezza minima della fattorizzazione; in particolare se n è un intero che ammette una fattorizzazione di lunghezza uno, ovvero $n = \pm p_1$, ed un'altra fattorizzazione di lunghezza s, ovvero $n = \pm q_1^{k_1} q_2^{k_2} \cdot \ldots \cdot q_s^{k_s}$, allora p_1 dividendo il prodotto dei q_i deve dividere uno dei fattori. Supponiamo che p_1 divida q_j; allora, essendo q_j irriducibile, deve essere $p_1 = q_j$ e quindi, per la legge di cancellazione

$$1 = \pm q_1^{k_1} q_2^{k_2} \cdot \ldots \cdot q_j^{k_j - 1} \cdot \ldots \cdot q_s^{k_s}$$

ma questo è possibile se, e solo se, s=1 e $n = \pm p_1 = \pm q_j$; pertanto la base dell'induzione è dimostrata.

In maniera del tutto analoga si ripete la dimostrazione supponendo che l'unicità della fattorizzazione sia vera per ogni intero che possiede una fattorizzazione di lunghezza $n - 1$ e dimostrandolo per l'intero generico che abbia una fattorizzazione di lunghezza n. ∎

Osservazione 1.1.5 Lo studente può facilmente dimostrare un risultato ben noto fin dalla scuola elementare: se $a = \pm p_1^{h_1} p_2^{h_2} \cdot \ldots \cdot p_t^{h_t}$ e $b = \pm q_1^{k_1} q_2^{k_2} \cdot \ldots \cdot q_s^{k_s}$, con p_i, q_j primi, allora il massimo comun divisore (a, b) è uguale al prodotto dei fattori primi comuni alle due fattorizzazioni presi ciascuno con il minimo esponente.

Esempio 1.1.2 Se consideriamo gli interi $a = 652$ e $b = 38$ dell'esempio precedente risulta $652 = 2^2 \cdot 163$ e $38 = 2 \cdot 19$ e, come già visto $(652, 38) = 2$.

Definizione 1.1.5 Se $a, b \in \mathbb{Z} \backslash \{0\}$ si definisce *minimo comune multiplo fra a e b*, e si denota $[a, b]$, un intero $m \in \mathbb{Z}$ tale che:

i) $m = as$, $m = bt$, $s, t \in \mathbb{Z}$;

ii) $c \in \mathbb{Z}$ / $c = as'$, $c = bt' \Rightarrow c = mk$, $k \in \mathbb{Z}$.

Osservazione 1.1.6 Come per il massimo comun divisore anche il minimo comune multiplo può essere considerato dal punto di vista della fattorizzazione e risulta che se $a = \pm p_1^{h_1} p_2^{h_2} \cdot \ldots \cdot p_t^{h_t}$ e $b = \pm q_1^{k_1} q_2^{k_2} \cdot \ldots \cdot q_s^{k_s}$, con p_i, q_j primi, allora il minimo comune multiplo $[a, b]$ è uguale al prodotto dei fattori primi comuni e non comuni alle due fattorizzazioni presi ciascuno con il massimo esponente.

Introduciamo ora un importante concetto di primalità relativa.

Definizione 1.1.6 Se a e b sono due interi non nulli si dice che a e b *sono coprimi* (*primi fra loro*) se $(a, b) = 1$.

Osservazione 1.1.7 Se a e b sono coprimi allora $\exists\ s, t \in \mathbb{Z}$ tali che $as + bt = 1$; inoltre, se $as + bt = 1$, per opportuni $s, t \in \mathbb{Z}$, allora a e b sono coprimi per quanto visto nella proposizione 1.1.2.

Esempio 1.1.3 Per ogni $a \in \mathbb{Z}\backslash\{0, -1\}$, a e $a + 1$ sono coprimi; infatti risulta $1 = (a + 1) \cdot 1 + a \cdot (-1)$.

Proposizione 1.1.5 *Se* $a = (a, b) \cdot a'$ *e* $b = (a, b) \cdot b'$, *allora* $(a', b') = 1$.

Dimostrazione - Risulta infatti

$$(a, b) = as + bt = (a, b)a's + (a, b)b't = (a, b)(a's + b't)$$

da cui $a's + b't = 1$. ∎

Dalla definizione di numero primo sappiamo che, se $p \in \mathbb{Z}$ è un numero primo e $ab = pz$, $z \in \mathbb{Z}$, allora $a = ph$ o $b = pk$, $h, k \in \mathbb{Z}$; vediamo ora cosa succede quando un intero divide un prodotto ed è coprimo con uno dei due fattori.

Proposizione 1.1.6 *Se* $a, b, c \in \mathbb{Z}\backslash\{0\}$, $ab = cz$, $z \in \mathbb{Z}$ *e* $(a, c) = 1$ *allora* $b = cw$, $w \in \mathbb{Z}$.

Dimostrazione - Poiché $(a, c) = 1$, risulta $1 = cx + ay$, $x, y \in \mathbb{Z}$; moltiplicando per b tale uguaglianza si ottiene $b = bcx + bay = bcx + czy = c(bx + zy)$. ∎

Come conseguenza della proposizione precedente possiamo dimostrare la seguente relazione fra minimo comune multiplo e massimo comun divisore.

Corollario 1.1.1 *Siano* a *e* b *due interi diversi da* 0 *e* ± 1, *allora risulta:*

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

Dimostrazione - Essendo $a = (a, b)a'$ e $b = (a, b)b'$, con $(a', b') = 1$, verifichiamo che $\dfrac{a \cdot b}{(a, b)} = (a, b)a'b'$ soddisfa alle condizioni del minimo comune multiplo fra a e b; innanzitutto ovviamente esso è un multiplo comune dei due interi.

Sia ora c un multiplo comune di a e b, verifichiamo che c è un multiplo di $(a, b)a'b'$; per l'ipotesi fatta esistono r e s tali che $c = ar = bs$ e pertanto risulta $c = (a, b)a'r = (a, b)b's$. Poiché $(a', b') = 1$, dalla proposizione precedente segue che a' divide s e b' divide r ovvero risulta, per opportuni h e k, $r = b'h$ e $s = a'k$ onde:

$$c = (a, b)a'r = (a, b)b's = c = (a, b)a'b'h = (a, b)b'a'k$$

e quindi in particolare $h = k$ e c è un multiplo di $(a, b)a'b'$, come volevamo dimostrare. ∎

Proposizione 1.1.7 *Se $a, b \in \mathbb{Z}$ sono divisori di $c \in \mathbb{Z}$ e $(a, b) = 1$, allora esiste $t \in \mathbb{Z}$ tale che $c = abt$.*

Dimostrazione - Risulta $c = as$, $s \in \mathbb{Z}$ e poiché b è un divisore di c, ovvero di as, essendo $(a, b) = 1$, per la proposizione precedente si ha che b è un divisore di s, onde $s = bt$ e quindi $c = as = abt$. ∎

Terminiamo questo paragrafo con alcuni risultati riguardanti l'insieme dei numeri primi.

Proposizione 1.1.8 *Esistono infiniti numeri primi.*

Dimostrazione - Supponiamo per assurdo che esistano solamente un numero finito di primi e siano essi $p_1, p_2, \ldots, p_k$; se consideriamo il numero intero $n = = (p_1 \cdot p_2 \cdot \ldots \cdot p_k) - 1$ risulta che n non è primo per l'ipotesi fatta, inoltre n non ammette fra i suoi fattori nessuno dei p_i. D'altra parte, per il teorema fondamentale dell'aritmetica, esso deve potersi esprimere come prodotto di primi e pertanto arriviamo ad una contraddizione dovuta al fatto di aver supposto che esistano solamente un numero finito di primi.

Chapter 2

GRUPPI

2.1 GRUPPI - PRIME PROPRIETÀ

In questo capitolo ci proponiamo di studiare la nozione di gruppo; premettiamo alcune definizioni.

Definizione 2.1.1 Sia H un insieme non vuoto; si definisce *operazione binaria* in H un'applicazione $* : H \times H \to H$ che associa ad ogni coppia ordinata di elementi di H un elemento di H.

Per comodità di notazione scriveremo, $\forall\ a, b \in H$, $a * b$ al posto di $*((a, b))$. Un insieme H dotato di un'operazione binaria $*$ si indica con il simbolo $(H, *)$. Esempi di operazioni sono ovviamente le usuali operazioni definite nell'insieme dei numeri razionali: $+$, $-$, $\cdot$ e la divisione $\div$ che è definita da $\mathbb{Q}\times\mathbb{Q}^*$ a $\mathbb{Q}$.

Osserviamo che $+$ e $\cdot$ sono definite anche in $\mathbb{N}$; mentre $-$ e $\div$ non sono definite in $\mathbb{N}$ in quanto, in generale, la differenza e il quoziente di due numeri naturali, quando abbia senso, non sono numeri naturali.

Nel seguito quando parleremo di un'operazione intenderemo sempre una operazione binaria.

Definizione 2.1.2 Un'operazione $* : H \times H \to H$ si dice *associativa* se, e solo se, $\forall\ a, b, c \in H$, risulta $(a * b) * c = a * (b * c)$.

Per quanto riguarda l'associatività possiamo osservare che, ad esempio in $\mathbb{Q}$, delle quattro usuali operazioni, $+, \cdot, -$ e $\div$, solo $+$ e $\cdot$ sono associative.

Definizione 2.1.3 Un'operazione $* : H \times H \to H$ si dice *commutativa* se, e solo se, $\forall\ a, b \in H$, risulta $a * b = b * a$.

Osservazione 2.1.1 Se un'operazione è associativa possiamo definire le potenze positive di un elemento; infatti, in tal caso, il risultato del prodotto $a*a*\ldots*a$ non dipende dall'ordine. Scriveremo quindi, $\forall\ n \in \mathbb{N}^*$, a^n al posto di $a * \ldots * a$, n volte, e parleremo della potenza n-esima di a (se l'operazione è espressa in forma additiva scriveremo na e parleremo di multiplo n-esimo di a).

Sempre come conseguenza della proprietà associativa è facile convincersi del fatto che, $\forall\ n, m \in \mathbb{N}$, risulta $a^n * a^m = a^{n+m} = a^{m+n} = a^m * a^n$ e $(a^n)^m = = a^{nm} = a^{mn} = (a^m)^n$; nel caso additivo risulterà $na * ma = (n+m)a = = (m+n)a = ma * na$ e $m(na) = (mn)a = (nm)a = n(ma)$.

Definizione 2.1.4 Un *gruppo* è un insieme non vuoto G, dotato di un'operazione $* : G \times G \to G$, tale che risultino verificate le seguenti proprietà:

1) l'operazione $*$ è associativa;

2) $\exists\ u \in G\ /\ \forall\ a \in G :\ a * u = u * a = a$;

3) $\forall\ a \in G\ \exists\ \tilde{a} \in G\ /\ a * \tilde{a} = \tilde{a} * a = u$.

Definizione 2.1.5 L'elemento u di cui al punto 2) della definizione di gruppo verrà chiamato *elemento neutro* di G rispetto a $*$; in particolare, se l'operazione in questione è detta moltiplicazione (addizione), si parlerà di *unità* (*zero*). Infine l'elemento $\tilde{a}$ è detto *il reciproco di* a e, nel caso particolare di moltiplicazione (addizione), si parlerà di *inverso* (*opposto*).

Definizione 2.1.6 *Un gruppo* $(G, *)$ *si dice commutativo o abeliano se l'operazione* $*$ *è commutativa. In altri termini se*

$$a * b = b * a \quad \forall\ a, b \in G$$

Iniziamo ad analizzare esempi familiari.

Esempio 2.1.1 Gli insiemi $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, sono tutti esempi di gruppo. Analizziamo in dettaglio il primo, $(\mathbb{Z},+)$. È chiaro che la somma di interi è associativa; l'elemento neutro è 0 e l'opposto di m è $-m$.

Un'altro esempio semplice ma importante è il seguente: sia K uno tra gli insiemi Z, Q, R; allora nell'insieme K^n delle n-ple ordinate di elementi di K

$$K^n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in K,\ 1 \leq i \leq n\}$$

si può definire un'operazione $+$ ponendo

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n).$$

Rispetto a tale operazione K^n risulta essere un gruppo: l'associatività dell'operazione segue facilmente dall'associatività dell'operazione in K; l'elemento neutro è $(0, 0, \ldots, 0)$, mentre l'inverso di $(x_1, x_2, \ldots, x_n)$ è $(-x_1, -x_2, \ldots, -x_n)$. Si osservi che in tutti gli esempi visti finora l'operazione è commutativa.

Esempio 2.1.2 Siano $A = \{1, 2, 3\}$ e $\mathcal{S}_3$ l'insieme delle applicazioni biiettive di A in A; allora l'insieme $\mathcal{S}_3$ è costituito dalle seguenti sei applicazioni:

$$\begin{array}{lll} id_A : A \to A & f_1 : A \to A & f_2 : A \to A \\ 1 \to 1 & 1 \to 2 & 1 \to 3 \\ 2 \to 2 & 2 \to 3 & 2 \to 1 \\ 3 \to 3 & 3 \to 1 & 3 \to 2 \end{array}$$

$$\begin{array}{lll} f_3 : A \to A & f_4 : A \to A & f_5 : A \to A \\ 1 \to 2 & 1 \to 3 & 1 \to 1 \\ 2 \to 1 & 2 \to 2 & 2 \to 3 \\ 3 \to 3 & 3 \to 1 & 3 \to 2 \end{array}$$

Descriviamo innanzitutto l'insieme $\mathcal{S}_3$ in modo più compatto scrivendo le applicazioni come tabelle in cui, nella seconda riga, sotto ogni elemento della prima riga scriviamo la sua immagine:

$$id_A = \begin{pmatrix} 1\ 2\ 3 \\ 1\ 2\ 3 \end{pmatrix}, \quad f_1 = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 3\ 1 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 1\ 2\ 3 \\ 3\ 1\ 2 \end{pmatrix},$$

$$f_3 = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 1\ 3 \end{pmatrix}, \quad f_4 = \begin{pmatrix} 1\ 2\ 3 \\ 3\ 2\ 1 \end{pmatrix}, \quad f_5 = \begin{pmatrix} 1\ 2\ 3 \\ 1\ 3\ 2 \end{pmatrix}.$$

Con semplici calcoli si può allora verificare che:

$$f_2 = f_1^{-1}, \quad f_3 = f_3^{-1}, \quad f_4 = f_4^{-1}, \quad f_5 = f_5^{-1};$$

inoltre, ad esempio,

$$(f_1 \circ f_3)(1) = f_1(f_3(1)) = f_1(2) = 3,$$

$$(f_1 \circ f_3)(2) = f_1(f_3(2)) = f_1(1) = 2,$$

$$(f_1 \circ f_3)(3) = f_1(f_3(3)) = f_1(3) = 1,$$

onde $f_1 \circ f_3 = f_4$.

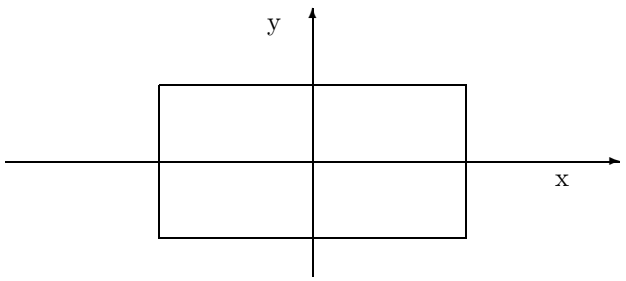
Lo studente si eserciti a calcolare gli altri prodotti possibili, e in particolare verifichi che $\mathcal{S}_3$ è un gruppo non abeliano, denominato *gruppo simmetrico su* 3 *elementi*

Vediamo un esempio di gruppo tratto dalla geometria.

Esempio 2.1.3 Consideriamo l'insieme dei movimenti rigidi di un rettangolo, ovvero delle trasformazioni del piano che portano il rettangolo in sé; siano x e y gli assi di simmetria del rettangolo, allora l'insieme dei movimenti rigidi del rettangolo è;

$$K = \{id,\ \sigma_x,\ \sigma_y,\ \rho_\pi\}$$

dove σ_x e σ_y sono le simmetrie rispetto ai due assi e ρ_π è la rotazione (oraria o antioraria) di angolo π.



Si verifica facilmente che K è un gruppo rispetto al prodotto di funzioni; a tale scopo costruiamo la tabella moltiplicativa:

$\circ$	id	σ_x	σ_y	ρ_π
id	id	σ_x	σ_y	ρ_π
σ_x	σ_x	id	ρ_π	σ_y
σ_y	σ_y	ρ_π	id	σ_x
ρ_π	ρ_π	σ_y	σ_x	id

Osserviamo che in questo gruppo ogni elemento è inverso di se stesso; ricordiamo che, essendo i movimenti rigidi particolari applicazioni del piano in se stesso, il prodotto operatorio è sicuramente associativo.

Il gruppo K viene detto *gruppo di Klein.*

D'ora in avanti la trattazione sarà relativa a gruppi in notazione moltiplicativa; tutto ciò che diremo si può riscrivere ovviamente per un gruppo in notazione additiva. Esplicitiamo gli assiomi di gruppo nelle due notazioni.

Notazione additiva

1) $(a+b)+c = a+(b+c) \quad \forall\, a, b\, c \in G.$

2) $\exists u \in G \mid a+u = u+a = a \quad \forall\, a \in G.$

3) $\forall a \in G\ \exists\, \tilde{a} \in G \mid a+\tilde{a} = \tilde{a}+a = u$

Notazione moltiplicativa

1) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall\, a, b\, c \in G.$

2) $\exists u \in G \mid a \cdot u = u \cdot a = a \quad \forall\, a \in G.$

3) $\forall a \in G\ \exists\, \tilde{a} \in G \mid a \cdot \tilde{a} = \tilde{a} \cdot a = u$

Per semplicità di notazione, tranne nei casi in cui risulterà indispensabile per la comprensione del testo, indicheremo sempre il risultato dell'operazione fra due elementi a e b con ab invece che con $a * b$ o $a \cdot b$.

Vediamo qualche proprietà che dipende dagli assiomi di gruppo

Proposizione 2.1.1 *In un gruppo G l'elemento neutro u è unico; inoltre u è l'unico elemento di G che coincide con il suo quadrato.*

Risulta poi che, $\forall\, a \in G$, l'inverso di a è unico.

Dimostrazione - Sia $e \in G$ un elemento tale che $\forall\ a \in G$ risulti $ae = ea = a$; allora, per le proprietà degli elementi e ed u, otteniamo $u = ue = e$.

Supponiamo ora che per l'elemento $g \in G$ valga la proprietà $g^2 = g$; allora moltiplicando per l'inverso di g otteniamo:

$$u = gg^{-1} = g^2g^{-1} = g.$$

Dimostriamo l'unicità dell'inverso per un elemento a di G; sia dunque a' un elemento di G tale che $aa' = a'a = u$. Allora risulta

$$a' = a'u = a'(a\tilde{a}) = (a'a)\tilde{a} = u\tilde{a} = \tilde{a}$$

e quindi a' è proprio $\tilde{a}$. ∎

Osservazione 2.1.2 Come conseguenza delle proprietà di unicità appena dimostrate, e imponendo la validità delle proprietà delle potenze $a^n * a^m = = a^{n+m}$ e $a^{nm} = (a^n)^m$, per n e m interi relativi qualsiasi, possiamo definire in un gruppo la potenza a^0 al modo seguente:

$$a^n * a^0 = a^n = a^n * u \implies a^0 = u.$$

Per quanto riguarda le potenze negative osserviamo che:

$$u = a^{(1-1)} = a * a^{-1} \implies a^{-1} = \tilde{a} \text{ l'inverso di } a.$$

Pertanto indicheremo sempre l'inverso di a con il simbolo a^{-1}; per un intero n qualsiasi risulterà allora:

$$a^{-n} = (a^{-1})^n.$$

Per l'inverso di un prodotto vale la seguente relazione:

Proposizione 2.1.2 *In un gruppo G, $\forall\ a, b \in G$, risulta $(ab)^{-1} = b^{-1}a^{-1}$.*

Dimostrazione - Essendo:

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aua^{-1} = u$$

per l'unicità dell'inverso deve essere $b^{-1}a^{-1} = (ab)^{-1}$. ∎

Osservazione 2.1.3 Dall'unicità dell'inverso segue che $a = (a^{-1})^{-1}$.

Definizione 2.1.7 Sia $(G, \cdot)$ un gruppo e sia S un sottoinsieme non vuoto di G; si dice che S è un *sottogruppo* di G se, e solo se, $(S, \cdot)$ è esso stesso un gruppo rispetto all'operazione indotta da G su S.

Se S è un sottogruppo di G scriveremo $S \leq$G.

Osservazione 2.1.4 Quando si dice che G induce un'operazione in S si intende dire che, $\forall\ a, b \in S$, $a \cdot b \in S$ ovvero che S è chiuso rispetto all'operazione di G.

Esempio 2.1.4 Consideriamo i seguenti tre sottoinsiemi del gruppo $(\mathbb{Z},+)$, $S = \mathbb{N}$, $R = \{-2, 0, 2\}$ e $T = 2\mathbb{Z} = \{2z : z \in \mathbb{Z}\}$; si verifica immediatamente che $\mathbb{Z}$ induce un'operazione in S e in T.

Dei due sottoinsiemi solo T, l'insieme dei numeri pari, è un sottogruppo; in S sono verificate tutte le proprietà di gruppo tranne l'esistenza del reciproco (dell'opposto).

Osserviamo che R contiene lo zero e l'opposto di ogni suo elemento ma non è un sottogruppo in quanto non è chiuso rispetto all'operazione di $\mathbb{Z}$; ad esempio $2 + 2 = 4 \notin R$.

Esempio 2.1.5 Un gruppo infinito può avere sottogruppi finiti; ad esempio nel gruppo $(\mathbb{Q}^*, \cdot)$ il sottoinsieme $S = \{1, -1\}$ è ovviamente un sottogruppo.

Osservazione 2.1.5 Un gruppo G, con elemento neutro u, possiede sempre almeno due sottogruppi: $\{u\}$ e G. I due sottogruppi coincidono se $G = \{u\}$.

Definizione 2.1.8 Se G è un gruppo con elemento neutro u, i sottogruppi $\{u\}$ e G si dicono *banali* e tutti gli eventuali sottogruppi diversi da questi si dicono *propri* o *non banali*.

Un utile criterio per verificare se un sottoinsieme di un gruppo è un sottogruppo è dato dalla seguente proposizione:

Proposizione 2.1.3 *Un sottoinsieme S di un gruppo $(G, \cdot)$ è un sottogruppo se, e solo se, S è non vuoto e, $\forall\, x, y \in S$, risulta $x \cdot y^{-1} \in S$.*

Dimostrazione - Come prima cosa osserviamo che, se S è un sottogruppo, esso è ovviamente non vuoto e la condizione dell'enunciato è ovviamente verificata.

Sia ora $S \subseteq G$, $S \neq \emptyset$, tale che $\forall\, x, y \in S$ risulti $x \cdot y^{-1} \in S$; dobbiamo verificare che S è chiuso rispetto al prodotto e che valgono le proprietà della definizione di gruppo. Innanzitutto, essendo $S \neq \emptyset$, esiste $x \in S$ e quindi $u = x \cdot x^{-1} \in S$; pertanto l'elemento neutro di G appartiene ad S. Vediamo ora che ogni elemento di S ha il suo inverso in S; infatti $\forall\, x \in S$, essendo $u, x \in S$, $x^{-1} = u \cdot x^{-1} \in S$.

Dobbiamo infine dimostrare che l'operazione di G è definita in S; risulta che, $\forall\, x, y \in S$, anche y^{-1} appartiene a S e quindi $x \cdot y = x \cdot (y^{-1})^{-1} \in S$.

L'operazione è sicuramente associativa, poiché G è un gruppo; abbiamo quindi dimostrato che S è un sottogruppo di G. ∎

Applicando il criterio precedente possiamo caratterizzare tutti i sottogruppi del gruppo $(\mathbb{Z},+)$.

Proposizione 2.1.4 *Sia S un sottoinsieme non vuoto di $(\mathbb{Z},+)$; allora S è un sottogruppo di $(\mathbb{Z},+)$ se, e solo se, $S = m\mathbb{Z} = \{mz : z \in \mathbb{Z}\}$, $m \in \mathbb{Z}$.*

Dimostrazione - Dimostriamo innanzitutto che $m\mathbb{Z}$ è un sottogruppo di $(\mathbb{Z},+)$; infatti, $\forall\, mz, mw \in m\mathbb{Z}$, risulta $mz - mw = m(z - w) \in m\mathbb{Z}$, onde $m\mathbb{Z}$ è un sottogruppo di $(\mathbb{Z},+)$.

Dimostriamo ora che, se S è un sottogruppo di $(\mathbb{Z},+)$, allora $\exists\, m \in \mathbb{Z}$ tale che $S = m\mathbb{Z}$. Sia dunque $S \leq \mathbb{Z}$; se S è il sottogruppo banale, costituito dal solo zero, allora ovviamente $S = 0{\cdot}\mathbb{Z}$. Se $S \neq \{0\}$ allora in S esiste almeno un elemento non nullo e, poiché in S ogni elemento ha il suo opposto, ad S appartiene almeno un intero positivo.

Sia dunque m il minimo positivo appartenente ad S, che esiste sicuramente per il principio del minimo in $\mathbb{N}$, e n un qualsiasi elemento di S; dividendo n per m si ottiene $n = mq + r$, $0 \leq r < m$, onde $r = n - mq$.

Se $q > 0$, $mq = m + \ldots + m$, q volte, onde $mq \in S$; analogamente, se $q < 0$, $mq = -m(-q) \in S$. In entrambi i casi risulta $r \in S$ e, per la minimalità di m in S, $r = 0$, onde $n = mq$; da ciò segue che $S = m\mathbb{Z}$. ∎

Se S e T sono due sottogruppi di un gruppo G allora la loro intersezione è sicuramente non vuota essendo $u \in S \cap T$; applicando il criterio della proposizione **??** possiamo dimostrare che tale intersezione è sempre un sottogruppo.

Esercizio 1 *L'intersezione $S \cap T$ di due sottogruppi S e T di un gruppo G è un sottogruppo di G.*

Dimostrazione - Abbiamo già osservato che $S \cap T \neq \emptyset$; siano ora $x, y \in S \cap T$ e quindi, per definizione di intersezione, $x, y \in S$ e $x, y \in T$; essendo poi S e T due sottogruppi risulta:

$$xy^{-1} \in S \;\text{ e }\; xy^{-1} \in T \implies xy^{-1} \in S \cap T$$

onde $S \cap T$ è un sottogruppo di G. ∎

Ci chiediamo se anche l'unione di due sottogruppi risulti essere un sottogruppo; la risposta è in generale negativa.

Esercizio 2 *L'unione $S \cup T$ di due sottogruppi S e T di un gruppo G è un sottogruppo di G se, e solo se coincide con uno dei due sottogruppi, ovvero se, e solo se, i due sottogruppi sono uno contenuto nell'altro.*

Dimostrazione - Possiamo verificare con un esempio che, in generale, l'unione di due sottogruppi non è un sottogruppo; in $\mathbb{Z}$ l'unione $2\mathbb{Z} \cup 3\mathbb{Z}$ è ovviamente diversa da $m\mathbb{Z}$ qualunque sia m.

Supponiamo ora che S e T siano sottogruppi di un gruppo G e che anche $S \cup T$ risulti essere un sottogruppo, vogliamo dimostrare che uno dei due, fra S e T, è contenuto nell'altro.

Supponiamo ad esempio che S non sia contenuto in T e dimostriamo che allora deve risultare $T \subseteq S$; essendo $S \nsubseteq T$ deve esistere $s \in S$ tale che $s \notin T$.

Vogliamo dimostrare che ogni elemento t di T appartiene a S; per la condizione di sottogruppo sappiamo che, essendo $S \cup T$ un sottogruppo, deve risultare $ts^{-1} \in S \cup T$ e pertanto, per la definizione di unione, $ts^{-1} \in S$ o $ts^{-1} \in T$.

Se fosse $ts^{-1} \in T$ allora l'elemento s^{-1} apparterrebbe a T, da cui $s \in T$ contro l'ipotesi, deve quindi essere $ts^{-1} \in S$ e quindi t appartiene ad S. ∎

Possiamo definire il sottogruppo unione di due sottogruppi utilizzando le proprietà dell'intersezione; premettiamo una definizione.

Definizione 2.1.9 Sia R un sottoinsieme di un gruppo G; definiamo *sottogruppo generato* da R e lo denotiamo con $< R >$ il minimo sottogruppo di G contenente R, ovvero il sottogruppo che si ottiene tramite l'intersezione di tutti i sottogruppi di G che contengono R, a partire da G stesso. Risulta quindi:

$$< R >= \bigcap_{R \subseteq H} H, \quad H \leq G.$$

Pertanto per due sottogruppi qualsiasi S e T potremo dare la definizione che segue.

Definizione 2.1.10 Siano S e T due sottogruppi di un gruppo G; definiamo *sottogruppo unione* di S e T e lo denotiamo con $< S \cup T >$ il sottogruppo di G generato dal sottoinsieme $S \cup T$. Risulta quindi:

$$< S \cup T >= \bigcap_{S,T \subseteq H} H, \quad H \leq G.$$

Esempio 2.1.6 Nel caso del gruppo $(\mathbb{Z},+\ )$ l'unione e l'intersezione di due sottogruppi assumono una forma particolare; risulta infatti che:

$$< m\mathbb{Z} \cup n\mathbb{Z} >= (m,n)\mathbb{Z} \quad \text{e} \quad m\mathbb{Z} \cap n\mathbb{Z} = [m,n]\mathbb{Z}$$

dove (m,n) e $[m,n]$ sono rispettivamente il massimo comun divisore e il minimo comune multiplo fra m e n.

Per convincerci di quanto affermato osserviamo che se $x \in m\mathbb{Z} \cap n\mathbb{Z}$ allora x deve essere contemporaneamente un multiplo di m e di n e pertanto deve essere un multiplo di $[m,n]$; viceversa ovviamente ogni multiplo di $[m,n]$ appartiene a $m\mathbb{Z} \cap n\mathbb{Z}$.

Per quanto riguarda l'unione osserviamo che il sottogruppo $< m\mathbb{Z} \cup n\mathbb{Z} >$ contiene le somme $mx + ny$, $x, y \in \mathbb{Z}$, e quindi, ricordando l'identità di Bézout, contiene il massimo comun divisore; pertanto il sottogruppo $(m,n)\mathbb{Z}$ è contenuto nel sottogruppo $< m\mathbb{Z} \cup n\mathbb{Z} >$.

L'uguaglianza segue dal fatto che $m\mathbb{Z}, n\mathbb{Z} \subseteq (m,n)\mathbb{Z}$ e dalla minimalità del sottogruppo unione.

Vogliamo introdurre e studiare una classe di gruppi abeliani finiti di particolare importanza. Per questo introduciamo in $\mathbb{Z}$ la seguente relazione di equivalenza.

Definizione 2.1.11 Sia $m \in \mathbb{Z}$, $m \geq 2$ e sia ρ la relazione così definita:

$$x \rho y \Leftrightarrow x - y = km,\ k \in \mathbb{Z}\ .$$

La relazione precedente prende il nome di *congruenza modulo m in $\mathbb{Z}$* e si scrive $a \equiv_m b$ ovvero $a \equiv b \bmod m$

Proposizione 2.1.5 *La relazione $\equiv_m$ è una equivalenza.*

Dimostrazione - Verifichiamo che la relazione è riflessiva, simmetrica e transitiva:

$\equiv_m$ è riflessiva : $\forall\ x \in\mathbb{Z},\ x - x = 0 \cdot m \Rightarrow x\rho x$

$\equiv_m$ è simmetrica : $x\rho y \Rightarrow x - y = k \cdot m \Rightarrow y - x = (-k) \cdot m \Rightarrow y\rho x$

$\equiv_m$ è transitiva : $x\rho y,\ y\rho z \Rightarrow x - y = k \cdot m,\ y - z = h \cdot m \Rightarrow$
$\Rightarrow x - z = (x - y) + (y - z) = (k + h) \cdot m \Rightarrow x\rho z.$ ∎

Per quanto riguarda la struttura delle classi di equivalenza di $\mathbb{Z}$ modulo m osserviamo che, potendo effettuare in $\mathbb{Z}$ la divisione euclidea, preso comunque $z \in\mathbb{Z}$ è possibile dividere z per m ottenendo un quoziente ed un resto in modo tale che:

$$z = mq + r, \quad 0 \leq r < m\ .$$

Da ciò segue che $z - r = mq$, onde $z \equiv r \bmod m$ e quindi $z \in [r]$.

In particolare possiamo dimostrare la seguente proposizione:

Proposizione 2.1.6 *In $\mathbb{Z}$ risulta $a \equiv b$ mod m se, e solo se, dividendo a e b per m si ottiene lo stesso resto.*

Dimostrazione - Supponiamo innanzitutto che sia $a \equiv b \bmod m$, $a = mq + r$ e $b = mq' + r'$, $0 \leq r, r' \leq m - 1$; dalle due uguaglianze precedenti otteniamo per sottrazione che

$$a - b = m(q - q') + (r - r') \text{ con } |r - r'| \leq m - 1$$

Poiché per ipotesi $a - b = km$ per un opportuno k intero, deve risultare $r - r' = 0$ ovvero $r = r'$.

Viceversa è immediato verificare che, se $a = mq + r$ e $b = mq' + r$, con $0 \leq r \leq m - 1$, risulta $a - b = m(q - q')$ ovvero $a \equiv b \bmod m$. ∎

Pertanto, ogni intero appartiene ad una di queste classi $\overline{0}, \overline{1}, \ldots, \overline{m-1}$, cioè le classi rappresentate dai possibili resti della divisione per m. Osserviamo poi che due resti diversi non possono mai essere congrui fra loro modulo m e quindi le classi distinte sono proprio in numero di m.

Definizione 2.1.12 La classe $\overline{r}$ si chiama *classe resto modulo m.*

Definizione 2.1.13 L'insieme quoziente $\mathbb{Z}/_{\equiv_m} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ viene detto *insieme delle classi resto modulo m* e si denota con $\mathbb{Z}_m$.

Osservazione 2.1.6 Ricordiamo che, per le note proprietà delle relazioni di equivalenza, risulta $a \equiv_m b$ se e solo se $\overline{a} = \overline{b}$.

Nell'insieme $\mathbb{Z}_m$ delle classi resto modulo m è possibile definire due operazioni fra classi, una di addizione e una di moltiplicazione, tramite i rappresentanti delle classi stesse al modo seguente:

$$\overline{a} + \overline{b} = \overline{a + b} \qquad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

Tale definizione però deve essere sottoposta ad una critica attenta (lo studente faccia molta attenzione a questo punto); infatti come è noto (cfr. osservazione **??**), se $a \equiv c \bmod m$ e $b \equiv d \bmod m$, allora $\overline{a} = \overline{c}$ e $\overline{b} = \overline{d}$.

Pertanto affinché la definizione data non dipenda dai particolari rappresentanti delle classi in questione, deve risultare $\overline{a+b} = \overline{c+d}$ e $\overline{a \cdot b} = \overline{c \cdot d}$.

Dimostriamo allora la seguente proprietà:

Proposizione 2.1.7 *Se $a \equiv c$ mod m e $b \equiv d$ mod m allora $\overline{a+b} = \overline{c+d}$ e $\overline{a \cdot b} = \overline{c \cdot d}$.*

Dimostrazione - Osserviamo che:

$$a \equiv c \bmod m \quad \Longleftrightarrow \quad a - c = k \cdot m$$

e

$$b \equiv d \bmod m \quad \Longleftrightarrow \quad b - d = h \cdot m$$

per opportuni h e k interi relativi.

Pertanto, per quanto riguarda la somma, risulta

$$(a+b) - (c+d) = (a-c) + (b-d) = (k+h) \cdot m$$

onde

$$a + b \equiv c + d \bmod m \quad \text{ e quindi } \quad \overline{a+b} = \overline{c+d}.$$

Per quanto riguarda il prodotto si procede in maniera analoga; moltiplichiamo rispettivamente per b e per c le due relazioni $a - c = k \cdot m$ e $b - d = h \cdot m$ e sommiamole, risulta:

$$a \cdot b - c \cdot b + b \cdot c - d \cdot c = a \cdot b - c \cdot d = (k \cdot b + h \cdot c) \cdot m$$

e quindi

$$a \cdot b \equiv c \cdot d \bmod \quad \text{ ovvero } \quad \overline{a \cdot b} = \overline{c \cdot d}. \ \blacksquare$$

Osservazione 2.1.7 Mostriamo su di un esempio che esistono relazioni di equivalenza su $\mathbb{Z}$ per le quali l'addizione in $\mathbb{Z}$ non induce una addizione fra classi di equivalenza; considerata la relazione di equivalenza ρ in $\mathbb{Z}$ associata alla partizione $\mathbb{Z}^- \cup \{0\} \cup \mathbb{Z}^+$ risulta:

$$-2 \rho - 5, \quad 2 \rho 3 \quad \text{ onde } \quad \overline{-2} = \overline{-5} \ \text{ e } \ \overline{2} = \overline{3} \quad \text{ ma } \quad -2 + 2 \not\rho - 5 + 3$$

e quindi non ha senso definire la somma $\overline{-2} + \overline{2} = \overline{0}$ essendo questa diversa da $\overline{-5} + \overline{3} = \overline{-2}$.

Lo studente provi a determinare una relazione su $\mathbb{Z}$ per la quale non si può definire la moltiplicazione fra classi

Definizione 2.1.14 *Si dice* **anello** *un insieme non vuoto A su cui sono definite due operazioni binarie $+$ e $\cdot$ che soddisfano le seguenti proprietà:*

1) (A,+) è un gruppo abeliano;

2) $\forall\ a,b,c \in A : a\cdot(b\cdot c) = (a\cdot b)\cdot c$
(proprietà assiciativa del prodotto);

3) $\forall\ a,b,c \in A : a\cdot(b+c) = a\cdot b + a\cdot c,\ (b+c)\cdot a = b\cdot a + c\cdot a$
(proprietà distributive del prodotto rispetto alla somma).

Definizione 2.1.15 *Un anello A si dice* **commutativo** *se il prodotto gode della proprietà commutativa; l'anello si dice* **unitario** *se esiste un elemento $u \in A$ tale che, $\forall\ a \in A$, $ua = au = a$.*

Relativamente alle operazioni definite in $\mathbb{Z}_m$ sussiste la seguente proposizione:

Proposizione 2.1.8 *$(\mathbb{Z}_m, +, \cdot)$ è un anello commutativo e unitario.*

Dimostrazione - Lasciamo le verifiche delle proprietà commutative, associative e distributive allo studente.

Per quanto riguarda l'operazione di addizione si ha che, $\forall\ \overline{a} \in \mathbb{Z}_m$:

$$\overline{a} + \overline{0} = \overline{0} + \overline{a} = \overline{a}$$

e

$$\overline{a} + (\overline{-a}) = (\overline{-a}) + \overline{a} = \overline{0}$$

onde $\overline{0}$ risulta essere l'elemento neutro per $(\mathbb{Z}_m, +)$ e $\overline{-a}$ l'opposto di $\overline{a}$.

Analogamente, per quanto riguarda l'operazione di moltiplicazione, risulta, $\forall\ \overline{a} \in \mathbb{Z}_m$:

$$\overline{a}\cdot\overline{1} = \overline{1}\cdot\overline{a} = \overline{a}$$

Pertanto abbiamo dimostrato che $(\mathbb{Z}_m, +, \cdot)$ è un anello commutativo e unitario. ∎

Osservazione 2.1.8 Relativamente alla sola struttura additiva, possiamo dire che $(\mathbb{Z}_m, +)$ è un gruppo commutativo.

Allo scopo di esaminare meglio la struttura di tale anello esaminiamo alcuni casi particolari.

Esempio 2.1.7 Costruiamo le tabelle della moltiplicazione in $(\mathbb{Z}_5, +, \cdot)$ e in $(\mathbb{Z}_6, +, \cdot)$; indicheremo con $\overline{a}$ le classi in $\mathbb{Z}_5$ e con $\tilde{a}$ le classi in $\mathbb{Z}_6$.

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\cdot$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$	$\tilde{3}$	$\tilde{4}$	$\tilde{5}$
$\tilde{0}$	$\tilde{0}$	$\tilde{0}$	$\tilde{0}$	$\tilde{0}$	$\tilde{0}$	$\tilde{0}$
$\tilde{1}$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$	$\tilde{3}$	$\tilde{4}$	$\tilde{5}$
$\tilde{2}$	$\tilde{0}$	$\tilde{2}$	$\tilde{4}$	$\tilde{0}$	$\tilde{2}$	$\tilde{4}$
$\tilde{3}$	$\tilde{0}$	$\tilde{3}$	$\tilde{0}$	$\tilde{3}$	$\tilde{0}$	$\tilde{3}$
$\tilde{4}$	$\tilde{0}$	$\tilde{4}$	$\tilde{2}$	$\tilde{0}$	$\tilde{4}$	$\tilde{2}$
$\tilde{5}$	$\tilde{0}$	$\tilde{5}$	$\tilde{4}$	$\tilde{3}$	$\tilde{2}$	$\tilde{1}$

.

Dalle due tabelle moltiplicative possiamo osservare che, mentre in $\mathbb{Z}_5$ non esistono classi $\overline{a}$ e $\overline{b}$, diverse dalla classe $\overline{0}$ tali che $\overline{a} \cdot \overline{b} = \overline{0}$, in $\mathbb{Z}_6$ esistono classi $\tilde{a}$ e $\tilde{b}$, diverse dalla classe $\overline{0}$, tali che $\tilde{a} \cdot \tilde{b} = \tilde{0}$.

Osserviamo inoltre che, in $\mathbb{Z}_5$ ogni classe non nulla ha un inverso, mentre in $\mathbb{Z}_6$, oltre all'elemento $\tilde{1}$, solamente $\tilde{5}$ ha inverso e risulta $\tilde{5} \cdot \tilde{5} = \tilde{1}$.

Possiamo quindi affermare che $(\mathbb{Z}_5 \backslash \{\overline{0}\}, \cdot)$ è un gruppo commutativo mentre $(\mathbb{Z}_6 \backslash \{\overline{0}\}, \cdot)$ non lo è.

Definizione 2.1.16 Un anello commutativo unitario $(A, +, \cdot)$ viene detto *campo* se in esso ogni elemento non nullo ammette inverso, ovvero:

$$\forall \quad a \in A \backslash \{0\} \quad \exists \quad a^{-1} \in A \quad \text{ tale che } \quad a \cdot a^{-1} = 1.$$

Esempio 2.1.8 Gli esempi più immediati di campo sono dati dai numeri razionali e dai numeri reali. Si verifichi per esercizio che l'insieme dei numeri reali del tipo $a + b\sqrt{2}$, con a, b razionali e operazioni

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$$

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (ac + 2bd) + (ad + bd)\sqrt{2}$$

risulta essere un campo.

Osservazione 2.1.9 Se $(A, +, \cdot)$ è un campo allora $(A, +)$ e $(A \backslash \{0\}, \cdot)$ sono due gruppi commutativi.

Definizione 2.1.17 Un elemento non nullo a di un anello commutativo $(A, +, \cdot)$ viene detto *divisore dello zero* se in A esiste un elemento non nullo b tale che risulti $a \cdot b = 0$.

Dall'esempio precedente si osserva che, fra $(\mathbb{Z}_5, +, \cdot)$ e $(\mathbb{Z}_6, +, \cdot)$, solo il primo risulta essere un campo; vediamo inoltre che nel primo non ci sono divisori dello zero mentre nel secondo gli elementi $\tilde{2}$, $\tilde{3}$ e $\tilde{4}$ sono divisori dello zero.

Vogliamo allora studiare la struttura dell'anello $(\mathbb{Z}_m, +, \cdot)$ per un modulo m qualsiasi; affrontiamo il problema ricordando quanto visto relativamente allo studio delle equazioni in congruenza.

Proposizione 2.1.9 *Un elemento non nullo $\overline{a}$ di $\mathbb{Z}_m$ è invertibile se, e solo se, l'intero a è coprimo con il modulo m.*

Dimostrazione - Affinché l'elemento $\overline{a}$ di $\mathbb{Z}_m$ sia invertibile deve esistere in $\mathbb{Z}_m$ un elemento $\overline{x}$ tale che:

$$\overline{a} \cdot \overline{x} = \overline{1} \quad \text{ ovvero } \quad a \cdot x \equiv 1 \bmod m \ .$$

D'altra parte tale equazione ammette soluzione se, e solo se, $(a, m) = 1$. Infatti, se $(a, m) = 1$, scrivendo l'identità di Bezout relativa ad a ed m otteniamo che esistono $r, s \in \mathbb{Z}$ tali che $1 = ar + ms$, onde $\overline{a} \cdot \overline{r} = \overline{1}$. Viceversa se la precedente congruenza ha soluzione $\overline{r}$, esiste $s \in \mathbb{Z}$ tale che $1 = ar + ms$, per cui $(a, m) = 1$. ∎

Corollario 2.1.1 *L'anello $(\mathbb{Z}_m, +, \cdot)$ è un campo se, e solo se, m è un numero primo.*

Esempio 2.1.9 In $\mathbb{Z}_{18}$ calcolare, se esiste, l'inverso di $\overline{7}$.

L'elemento $\overline{7}$ ammette inverso in quanto 7 è coprimo con 18; scriviamo l'identità di Bézout relativa agli interi 7 e 18, applicando l'algoritmo delle divisioni successive, si ha

$$18 = 7 \cdot 2 + 4, \quad 7 = 4 \cdot 1 + 3, \quad 4 = 3 \cdot 1 + 1$$

da cui

$$1 = 4 + 3 \cdot (-1) = 4 + (7 + 4 \cdot (-1)) \cdot (-1) = 7 \cdot (-1) + 4 \cdot 2 =$$

$$= 7 \cdot (-1) + (18 + 7 \cdot (-2)) \cdot 2 = 18 \cdot (2) + 7 \cdot (-5)$$

Passando alle classi modulo 18, risulta:

$$\overline{1} = \overline{18} \cdot \overline{2} + \overline{7} \cdot \overline{-5} = \overline{7} \cdot \overline{13}.$$

ovvero

$$\overline{7}^{-1} = \overline{13}.$$

Osservazione 2.1.10 Denotiamo con $\varphi(m)$ il numero degli interi positivi minori di m e primi con m. Osserviamo che, per quanto visto nel paragrafo precedente, l'anello $(\mathbb{Z}_m, +, \cdot)$ contiene esattamente $\varphi(m)$ elementi invertibili; denotiamo con $\mathbb{U}_m = \{\overline{a} \ : \ (a, m) = 1\}$ l'insieme degli elementi invertibili di $\mathbb{Z}_m$.

Definizione 2.1.18 Un elemento invertibile di $\mathbb{Z}_m$ viene detto *unità di* $\mathbb{Z}_m$.

Proposizione 2.1.10 *L'insieme delle unità di $\mathbb{Z}_m$ rispetto al prodotto, ovvero $(\mathbb{U}_m, \cdot)$, è un gruppo commutativo.*

Dimostrazione - Basta dimostrare che il prodotto di due elementi invertibili è ancora invertibile, ma questo si verifica facilmente, ad esempio osservando che, se $(a, m) = 1$ e $(b, m) = 1$ allora ovviamente $(ab, m) = 1$. ■

Corollario 2.1.2 *Se p è un numero primo, $\mathbb{U}(p)$=$\mathbb{Z}_p^*$ e pertanto possiamo affermare che $(\mathbb{Z}_p^*, \cdot)$ è un gruppo.*

Nel caso in cui il modulo non è un numero primo i divisori dello zero sono caratterizzati dalla seguente proposizione:

Proposizione 2.1.11 *Un elemento non nullo $\overline{a} \in \mathbb{Z}_m$, dove m non è primo, è un divisore dello zero se, e solo se, l'intero a non è coprimo con il modulo m.*

Dimostrazione - Se $(a, m) = d$, $d \neq 1$, allora $a = da'$ e $m = dm'$ e quindi:

$$\overline{m'} \neq \overline{0} \quad \text{e} \quad \overline{a} \cdot \overline{m'} = \overline{m} \cdot \overline{a'} = \overline{0}.$$

Viceversa, se esiste elemento non nullo $\overline{b}$ tale che risulti $\overline{a} \cdot \overline{b} = \overline{0}$, questo implica che m divide ab; inoltre, essendo la classe $\overline{b}$ non nulla, m non divide b.

Sia dunque p un primo che divide m e non divide b; allora p divide a e quindi $(a, m) \neq 1$. ∎

Esempio 2.1.10 Determiniamo tutti gli elementi invertibili e tutti i divisori dello zero dell'anello $(\mathbb{Z}_{12}, +, \cdot)$.

Per quanto appena dimostrato gli elementi invertibili di $(\mathbb{Z}_{12}, +, \cdot)$, diversi da $\overline{1}$, sono $\overline{5}$, $\overline{7}$ e $\overline{11}$; risulta infatti

$$\overline{5} \cdot \overline{5} = \overline{25} = \overline{1}, \quad \overline{7} \cdot \overline{7} = \overline{49} = \overline{1}, \quad \overline{11} \cdot \overline{11} = \overline{121} = \overline{1}$$

ovvero ogni elemento è inverso di se stesso.

I restanti elementi non nulli sono divisori dello zero e risulta, ad esempio:

$$\overline{2} \cdot \overline{6} = \overline{0}, \quad \overline{3} \cdot \overline{4} = \overline{0}, \quad \overline{8} \cdot \overline{9} = \overline{0}, \quad \overline{10} \cdot \overline{6} = \overline{0}.$$

2.2 CLASSI LATERALI

Cerchiamo di approfondire le nostre conoscenze relative ai sottogruppi di un gruppo. In particolare vediamo come, a partire da un sottogruppo, è possibile definire nel gruppo due relazioni di equivalenza; a questo scopo osserviamo che, nel gruppo $\mathbb{Z}$, la congruenza modulo m si può enunciare al modo seguente:

$$a \equiv b \bmod m \quad \Longleftrightarrow \quad a - b \in m\mathbb{Z}.$$

Proposizione 2.2.12 *Siano G un gruppo, S un suo sottogruppo, ρ e ρ' le relazioni definite in G al modo seguente:*

$$\forall\ a, b \in G : a\rho b \Longleftrightarrow a^{-1}b \in S, \quad a\rho' b \Longleftrightarrow ba^{-1} \in S$$

allora ρ e ρ' sono relazioni di equivalenza che prendono il nome di relazioni indotte da S in G.

Dimostrazione - La relazione ρ gode della proprietà riflessiva; infatti, $\forall\ a \in G$, risulta $a^{-1}a = u \in$S.

Se poi $a\rho b$, onde $a^{-1}b \in S$, essendo S un sottogruppo e contenendo quindi l'inverso di ogni suo elemento, risulta $b^{-1}a = (a^{-1}b)^{-1} \in S$ e pertanto $b\rho a$; da ciò segue che ρ verifica la proprietà simmetrica.

Infine, per quanto riguarda la proprietà transitiva, se $a\rho b$ e $b\rho c$, si ha che $a^{-1}b, b^{-1}c \in S$, onde $a^{-1}c = (a^{-1}b)(b^{-1}c) \in S$, poiché S è chiuso rispetto al prodotto; quindi $a\rho c$ e pertanto ρ è transitiva.

Abbiamo così dimostrato che ρ è una relazione di equivalenza; in modo del tutto analogo si dimostra che ρ' è di equivalenza. ∎

Come è noto, ad ogni relazione di equivalenza su un insieme A si può associare una partizione di A; studiamo allora la struttura delle partizioni associate alle relazioni ρ e ρ' della proposizione precedente.

Proposizione 2.2.13 *Se G è un gruppo, S un suo sottogruppo, ρ e ρ' le relazioni di equivalenza indotte da S in G, $\forall\ a \in G$ risulta*

$$[a]_\rho = aS = \{as \ / \ s \in S\},$$

$$[a]_{\rho'} = Sa = \{sa \ / \ s \in S\}.$$

Dimostrazione - Per quanto riguarda la partizione associata alla relazione ρ si ha:

$$b \in [a]_\rho \iff a^{-1}b \in S \iff a^{-1}b = s \in S \iff b = as \in aS$$

onde $[a]_\rho = aS$.

In modo analogo si dimostra che $[a]_{\rho'} = Sa$. ∎

Definizione 2.2.19 Sia S un sottogruppo di un gruppo G; definiamo *classe laterale destra* (*sinistra*) relativa all'elemento a, l'insieme $Sa = \{sa : s \in S\}$ ($aS = \{as : s \in S\}$).

Osservazione 2.2.11 Due classi laterali destre (sinistre), essendo classi di equivalenza, o coincidono o sono disgiunte. Inoltre, essendo l'insieme delle classi laterali destre (sinistre) una partizione del gruppo, la loro unione risulta essere tutto il gruppo.

Osservazione 2.2.12 Il sottogruppo S è una classe laterale destra (sinistra) avente l'elemento neutro come uno dei suoi rappresentanti; inoltre, poiché ogni sottogruppo deve contenere l'elemento neutro e poiché due classi distinte sono disgiunte, S è l'unica classe laterale che risulta essere un sottogruppo.

Possiamo ora dimostrare che le classi laterali sono fra loro equipotenti. Inoltre le due partizioni, in classi laterali destre e in classi laterali sinistre, sono anche esse equipotenti.

Proposizione 2.2.14 *Siano G un gruppo e S un suo sottogruppo; allora esiste una biiezione tra una qualsiasi classe laterale destra (sinistra) e S. In particolare, se S è un sottogruppo di G contenente m elementi, ogni classe laterale destra (sinistra) contiene m elementi.*

Dimostrazione - Sia $\varphi : S \to Sa$ l'applicazione definita ponendo, $\forall\ s \in S$, $\varphi(s) = sa$; allora se $\varphi(s) = \varphi(s')$ si ha $sa = s'a$ e quindi, moltiplicando a destra per a^{-1}, risulta $s = s'$, onde φ è iniettiva.

Inoltre, $\forall\ s''a \in Sa$, risulta $s''a = \varphi(s'')$, onde φ è suriettiva; pertanto φ è una biiezione. L'ultima parte dell'enunciato è una ovvia conseguenza di quanto appena dimostrato. ∎

Proposizione 2.2.15 *Siano G un gruppo, S un suo sottogruppo, P e P' le partizioni associate rispettivamente alle relazioni ρ e ρ'; allora l'applicazione $\psi : P \to P'$ che alla classe aS associa la classe Sa^{-1} è una biiezione.*

Dimostrazione - Cominciamo innanzitutto con il dimostrare che ψ è ben definita, ovvero non dipende dalla scelta del rappresentante della classe stessa; a tal fine sia $a\rho b$, ovvero $b \in aS$, onde $b = as$, $s \in S$. Da ciò segue che $b^{-1} = s^{-1}a^{-1}$ e quindi $b^{-1} \in Sa^{-1}$; pertanto $Sa^{-1} = Sb^{-1}$ da cui segue la buona definizione di ψ.

Per quanto riguarda l'iniettività di ψ, se $Sx^{-1} = Sy^{-1}$, allora, per ogni $s \in S$, esiste $s' \in S$ tale che $sx^{-1} = s'y^{-1}$, onde $x^{-1} = s^{-1}s'y^{-1}$ e quindi $x = ys'^{-1}s \in yS$; da ciò segue che $xS = yS$ e pertanto ψ è iniettiva.

Essendo poi, per ogni Sz in P', $Sz = \psi(z^{-1}S)$, abbiamo che ψ è suriettiva, onde l'asserto. ∎

Osservazione 2.2.13 La proposizione precedente ci permette di asserire che, se P (P') ha un numero finito di elementi, allora P' (P) ha lo stesso numero di elementi.

Definizione 2.2.20 Dato un sottogruppo S di un gruppo G chiamiamo *indice* di S in G la cardinalità di P (nel caso finito diremo il numero delle classi laterali destre (sinistre)) e scriviamo $i = [G : S]$.

Come conseguenza dei risultati precedenti si può dimostrare il seguente teorema:

Proposizione 2.2.16 (Teorema di Lagrange) *Se G è un gruppo contenente n elementi ed S un suo sottogruppo contenente m elementi, allora $n = mi$, dove i è l'indice di S in G.*

Dimostrazione - Siano $Sa_1, \ldots, Sa_i$ le classi laterali destre distinte, onde $G = Sa_1 \cup \ldots \cup Sa_i$ e $Sa_u \cap Sa_v = \emptyset$ se $u \neq v$; per quanto dimostrato nella proposizione **??**, ogni classe laterale destra contiene esattamente m elementi, onde $n = mi$ come richiesto.

Il caso delle classi laterali sinistre è ovviamente analogo. ∎

Corollario 2.2.3 *Sia G un gruppo avente p elementi, con p primo; allora gli unici sottogruppi di G sono quelli banali.*

Dimostrazione - L'asserto è conseguenza del teorema di Lagrange e del fatto che gli unici divisori positivi di p sono 1 e p . ∎

Osservazione 2.2.14 Osserviamo che, se G è un gruppo contenente n elementi e m è un divisore di n, il teorema di Lagrange non ci assicura che esista un sottogruppo di G contenente m elementi; vedremo nel seguito un esempio in tal senso.

Definizione 2.2.21 Se G è un gruppo contenente n elementi, il numero naturale n si dice *ordine* di G.

Definizione 2.2.22 Sia G un gruppo con elemento neutro u; se $g \in G$ ed esiste $k \in \mathbb{Z}$, $k \neq 0$, tale che $g^k = u$, si definisce *periodo* o *ordine* dell'elemento g, e si denota con $o(g)$, il minimo intero positivo h tale che $g^h = u$.

Motiviamo ora il fatto di chiamare con lo stesso nome 'ordine' due cose diverse; per l'ordine di un elemento valgono le seguenti proprietà:

Proposizione 2.2.17 *Se G è un gruppo, u il suo elemento neutro e $g \in G$ un elemento di periodo h, allora:*
1) u è l'unico elemento di periodo uno;
2) $g^k = u \iff h$ divide k, $t \in \mathbb{Z}$;
3) $o(g) = o(g^{-1})$.

Dimostrazione - 1) Se $g^1 = u$, ovviamente $g = u$.
2) Dividendo k per h si ottiene $k = hq + r$, $0 \leq r < h$; pertanto

$$g^k = u \Longleftrightarrow g^{ht+r} = u \Longleftrightarrow g^{ht}g^r = u \Longleftrightarrow g^r = u \Longleftrightarrow r = 0 \Longleftrightarrow k = hq$$

dove la penultima implicazione dipende dalla minimalità di h come periodo di g; pertanto $g^k = u$ se, e solo se, k è un multiplo di h.
3) Se $o(g) = h$ e $o(g^{-1}) = k$, allora $g^h = u$ e $(g^{-1})^k = u$, onde $(g^{-1})^h = (g^h)^{-1} = u$ e $g^k = [(g^{-1})^k]^{-1} = u$ e pertanto, per la 2), $h = kt'$ e $k = ht$ e questo implica $h = k$. ∎

Introduciamo ora un particolare tipo di sottogruppi.

Proposizione 2.2.18 *Sia g un elemento di un gruppo G; allora il sottoinsieme $< g >= \{g^t \ / \ t \in \mathbb{Z}\}$ è un sottogruppo che coincide con il sottogruppo generato da $\{g\}$. Se poi g ha ordine s allora $< g >$ ha ordine s .*

Dimostrazione - Per dimostrare che $< g >$ è un sottogruppo utilizziamo il criterio visto nella proposizione **??**; osserviamo innanzitutto che $< g >$ è non vuoto poiché contiene g.

Considerati ora due elementi qualsiasi g^h e g^k di $< g >$, risulta $g^h(g^k)^{-1} = g^{h-k} \in < g >$ e pertanto $< g >$ è un sottogruppo di G. L'affermazione che tale sottogruppo è il minimo che contenga g è ovvia in quanto in un sottogruppo il prodotto di due elementi deve appartenere ancora al sottogruppo stesso.

Per dimostrare che, se g ha ordine s, allora il sottogruppo $< g >$ ha s elementi dimostriamo che ogni potenza di g si può scrivere come g^t con $t = 0, 1, \ldots, s-1$; infatti, se $g^h = g^k$, $h \neq k$, allora $g^{h-k} = u$ e, per la 2) della proposizione precedente, si ha che $h - k = sq$, ovvero che $h \equiv k \bmod s$.

Pertanto due potenze di g sono lo stesso elemento se, e solo se, gli esponenti appartengono alla stessa classe di equivalenza modulo s; otteniamo quindi che $< g >= \{u = g^0, g^1, \ldots, g^{s-1}\}$. ∎

Corollario 2.2.4 *Se G è un gruppo di ordine n e g è un elemento di G, allora $o(g)$ divide n.*

Dimostrazione - Poiché $o(g)$ è l'ordine del sottogruppo $< g >$, l'asserto segue dal teorema di Lagrange. ∎

Esercizio 3 *Un gruppo G di ordine pari contiene sempre un numero dispari di elementi di ordine due.*

Dimostrazione - Innanzitutto osserviamo che un elemento diverso da u è di periodo due se, e solo se, coincide con il proprio inverso; d'altra parte, come conseguenza del teorema di Lagrange, un gruppo di ordine dispari non può avere elementi di ordine due.

Sia G un gruppo contenente $2n$ elementi e $G = \{u\} \cup H \cup K$ dove H è il sottoinsieme di G contenente tutti gli elementi che non coincidono con il proprio inverso e K è il sottoinsieme degli elementi di periodo due. Vogliamo dimostrare che K è non vuoto e di cardinalità dispari; se H è vuoto questo è ovvio in quanto risulta $|K| = 2n - 1$.

Supponiamo quindi che H sia non vuoto; allora esso può essere ripartito in coppie di elementi che sono uno l'inverso dell'altro.

Risulta quindi $|H| = 2h$ onde $|K| = 2(n - h) - 1$. ∎

Esempio 2.2.11 Determiniamo i periodi degli elementi di $(\mathbb{Z}_{18}, +)$; sappiamo già che $o(\overline{0}) = 1$. Risulta poi $18 \cdot \overline{1} = \overline{18} = \overline{0}$ e 18 è ovviamente il più piccolo intero positivo che verifica questa proprietà, onde $o(\overline{1}) = 18$.

Per quanto riguarda $\overline{2}$ si ha $9 \cdot \overline{2} = \overline{18} = \overline{0}$; inoltre, poiché per $0 < h < 9$ risulta $h \cdot \overline{2} = \overline{2h} \neq \overline{0}$, $o(\overline{2}) = 9$. Lo studente può facilmente verificare che i periodi degli altri elementi sono:

$$o(\overline{9}) = 2, \quad o(\overline{6}) = o(\overline{12}) = 3, \quad o(\overline{3}) = o(\overline{15}) = 6,$$

$$o(\overline{2}) = o(\overline{4}) = o(\overline{8}) = o(\overline{10}) = o(\overline{14}) = o(\overline{16}) = 9,$$

$$o(\overline{5}) = o(\overline{7}) = o(\overline{11}) = o(\overline{13}) = o(\overline{17}) = o(\overline{1}) = 18.$$

Torniamo ora ad occuparci di classi laterali e osserviamo che, se un gruppo G è commutativo, le classi laterali destre coincidono con quelle sinistre; infatti $\forall$ $a \in G$ e $\forall$ $s \in S$, risulta $as = sa$. Ci chiediamo allora se, dato un gruppo G non commutativo e un suo sottogruppo S, è possibile che le classi laterali destre e sinistre coincidano, ovvero che, $\forall$ $a \in G$, risulti $aS = Sa$. Questo naturalmente non significa che, $\forall$ $s \in S$, risulta $as = sa$, ma che, $\forall$ $s \in S$, $\exists$ $s' \in S$ tale che $as = s'a$. Mostriamo con un esempio che questo è possibile.

Esempio 2.2.12 L'insieme delle permutazioni su tre elementi:

$$\mathcal{S}_3 = \left\{ id, \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 312 \end{pmatrix}, \begin{pmatrix} 123 \\ 132 \end{pmatrix}, \begin{pmatrix} 123 \\ 321 \end{pmatrix}, \begin{pmatrix} 123 \\ 213 \end{pmatrix} \right\},$$

visto nell'esempio **??**, è un gruppo non commutativo relativamente all'operazione di prodotto operatorio, come si verifica facilmente; in tale gruppo il sottoinsieme:

$$R = \left\{ id, \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 312 \end{pmatrix} \right\}$$

costituisce un sottogruppo, come subito si verifica.

Per quanto riguarda le classi laterali possiamo calcolarle e si ha:

$$\begin{pmatrix} 123 \\ 213 \end{pmatrix} \circ R = \left\{ \begin{pmatrix} 123 \\ 213 \end{pmatrix} \circ id, \begin{pmatrix} 123 \\ 213 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 213 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 312 \end{pmatrix} \right\} =$$

$$= \left\{ \begin{pmatrix} 123 \\ 213 \end{pmatrix}, \begin{pmatrix} 123 \\ 132 \end{pmatrix}, \begin{pmatrix} 123 \\ 321 \end{pmatrix} \right\} ;$$

d'altra parte

$$R \circ \begin{pmatrix} 123 \\ 213 \end{pmatrix} = \left\{ id \circ \begin{pmatrix} 123 \\ 213 \end{pmatrix}, \begin{pmatrix} 123 \\ 231 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 213 \end{pmatrix}, \begin{pmatrix} 123 \\ 312 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 213 \end{pmatrix} \right\} =$$

$$= \left\{ \begin{pmatrix} 123 \\ 213 \end{pmatrix}, \begin{pmatrix} 123 \\ 321 \end{pmatrix}, \begin{pmatrix} 123 \\ 132 \end{pmatrix} \right\},$$

e quindi

$$\begin{pmatrix} 123 \\ 213 \end{pmatrix} \circ R = R \circ \begin{pmatrix} 123 \\ 213 \end{pmatrix} \ .$$

Osserviamo che, poiché le classi laterali costituiscono una partizione, deve essere:

$$\begin{pmatrix} 123 \\ 213 \end{pmatrix} \circ R = \begin{pmatrix} 123 \\ 321 \end{pmatrix} \circ R = \begin{pmatrix} 123 \\ 132 \end{pmatrix} \circ R =$$

$$= R \circ \begin{pmatrix} 123 \\ 213 \end{pmatrix} = R \circ \begin{pmatrix} 123 \\ 321 \end{pmatrix} = R \circ \begin{pmatrix} 123 \\ 132 \end{pmatrix}$$

e

$$R = id \circ R = \begin{pmatrix} 123 \\ 231 \end{pmatrix} \circ R = \begin{pmatrix} 123 \\ 312 \end{pmatrix} \circ R =$$

$$= R \circ id = R \circ \begin{pmatrix} 123 \\ 231 \end{pmatrix} = R \circ \begin{pmatrix} 123 \\ 312 \end{pmatrix}.$$

Osserviamo infine che, nello stesso gruppo, esiste almeno un sottogruppo per il quale le classi laterali destre e sinistre non coincidono; infatti, se $T = \left\{ id, \begin{pmatrix} 123 \\ 213 \end{pmatrix} \right\}$, allora T è un sottogruppo di $\mathcal{S}_3$ e risulta

$$\begin{pmatrix} 123 \\ 231 \end{pmatrix} \circ T = \left\{ \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 321 \end{pmatrix} \right\} \neq T \circ \begin{pmatrix} 123 \\ 231 \end{pmatrix} = \left\{ \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 132 \end{pmatrix} \right\}.$$

Definizione 2.2.23 Un sottogruppo N di un gruppo G si dice *normale* se, e solo se, $\forall\, g \in G$, risulta $gN = Ng$. Per indicare che N è un sottogruppo normale di G si scrive $N \lhd G$.

Osservazione 2.2.15 Ovviamente tutti i sottogruppi di un gruppo commutativo sono normali. Osserviamo inoltre che il sottogruppo R dell'esempio precedente è normale in $\mathcal{S}_3$; tale sottogruppo è di indice due ed è immediato dimostrare che questa condizione è sufficiente per la normalità.

Proposizione 2.2.19 *In un gruppo G ogni sottogruppo N di indice due è normale.*

Dimostrazione - Se $[G : N] = 2$ allora le due partizioni in classi laterali destre e sinistre coincidono, essendo uguali a $\{N, G\backslash N\}$. ∎

Per verificare la normalità di un sottogruppo risulta utile la seguente caratterizzazione.

Proposizione 2.2.20 *Condizione necessaria e sufficiente affinché un sottogruppo N sia normale in G è che:*

$$\forall\, x \in N \ \ e \ \forall\, g \in G \ \ \textit{risulta} \ \ gxg^{-1} \in N.$$

Dimostrazione - Supponiamo che $N \lhd G$; allora, per definizione di sottogruppo normale, $\forall\, g \in G$ risulta $gN = Ng$. Questo implica che $\forall\, x \in N$ esiste $x' \in N$ tale che $gx = x'g$ ovvero $gxg^{-1} = x'$; pertanto la condizione è necessaria.

Vediamo ora che la condizione è anche sufficiente; se, $\forall\, x \in N$ e $\forall\, g \in G$, l'elemento gxg^{-1} appartiene a N allora esiste $x' \in N$ tale che $gxg^{-1} = x'$, ovvero $gx = x'g$. Pertanto $\forall\, g \in G$ risulta $gN = Ng$, onde $N \lhd G$. ∎

Osservazione 2.2.16 Se N è un sottogruppo normale di un gruppo G, allora le due relazioni di equivalenza ρ e ρ', corrispondenti alle partizioni in classi laterali destre e sinistre, coincidono e il relativo insieme quoziente verrà denotato con il simbolo G/N.

Alla luce dell'osservazione precedente possiamo dire che $\mathbb{Z}_m$, l'insieme delle classi di equivalenza modulo la relazione di congruenza, è uguale a $\mathbb{Z}/m\mathbb{Z}$.

In tale insieme era stato possibile definire le operazioni di addizione e moltiplicazione tramite i rappresentanti delle classi, dimostrando che la definizione non dipendeva dai particolari rappresentanti scelti; vediamo che possiamo fare la stessa cosa nell'insieme quoziente G/N, quando N è un sottogruppo normale.

Proposizione 2.2.21 *Se N è un sottogruppo normale di un gruppo G, è possibile definire un'operazione nell'insieme G/N al modo seguente:*

$$\forall\ gN, hN \in G/N, \quad gN \cdot hN = ghN;$$

relativamente a questa operazione G/N è un gruppo, che prende il nome di gruppo quoziente di G modulo N.

Dimostrazione - Dobbiamo verificare innanzitutto che l'operazione è ben definita, ovvero che non dipende dalla scelta dei rappresentanti delle classi; a tale scopo verifichiamo che, presi comunque un elemento in gN ed uno in hN, il loro prodotto appartiene a ghN.

Siano dunque $g', h' \in G$ tali che $g' \in gN$ e $h' \in hN$; questo implica che $g' = gn_1$ e $h' = hn_2$ per opportuni n_1, n_2 in N. Risulta allora:

$$g'h' = (gn_1)(hn_2) = g(n_1h)n_2 = g(hn_3)n_2 = ghn_4 \in ghN$$

dove $n_1h = hn_3$, per un opportuno $n_3 \in N$, per la normalità di N.

A questo punto verifichiamo che $(G/N, \cdot)$ è un gruppo; tale verifica è immediata in quanto l'operazione in G/N è definita sui rappresentanti delle classi e tali rappresentanti appartengono ad un gruppo. In particolare $\cdot$ è associativa in quanto, $\forall\ g, h, k \in G$:

$$gN \cdot (hN \cdot kN) = gN \cdot hkN = g(hk)N = (gh)kN = ghN \cdot kN = (gN \cdot hN) \cdot kN;$$

inoltre ovviamente la classe $uN = N$ risulta essere l'elemento neutro in G/N e l'inverso della classe gN è la classe $g^{-1}N$. ∎

Osservazione 2.2.17 Vale la pena osservare che, poiché l'operazione fra classi non dipende dalla scelta dei rappresentanti delle classi stesse, se $gN = hN$ allora $g^{-1}N = h^{-1}N$ e quindi la classe $g^{-1}N$ sarà costituita da tutti, e soli, gli inversi degli elementi della classe gN.

Esempio 2.2.13 Consideriamo il gruppo $(\mathbb{Z}_6, +)$ e determiniamo i suoi sottogruppi e i suoi quozienti.

Sappiamo che $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ e che $\{\overline{0}\}$ e $\mathbb{Z}_6$ sono i due sottogruppi banali; inoltre per il teorema di Lagrange i sottogruppi non banali possono avere 2 o 3 elementi.

Osserviamo poi che un sottogruppo con due elementi deve contenere $\overline{0}$ e un elemento che coincide con il suo opposto, mentre un sottogruppo con tre

elementi deve contenere, oltre a $\overline{0}$, due elementi di ordine tre. Con semplici calcoli si trovano allora i seguenti sottogruppi non banali

$$H = \{\overline{0}, \overline{3}\} \quad \text{e} \quad K = \{\overline{0}, \overline{2}, \overline{4}\}$$

I sottogruppi H e K sono ovviamente normali, poiché $\mathbb{Z}_6$ è commutativo, e quindi possiamo considerare i gruppi quoziente $\mathbb{Z}_6/H$ e $\mathbb{Z}_6/K$; indicheremo con $[\overline{a}]_H$ la classe $\overline{a} + H$ e analogamente con $[\overline{a}]_K$ la classe $\overline{a} + K$.

Risulta allora:

$$\mathbb{Z}_6/H = \{[\overline{0}]_H, [\overline{1}]_H, [\overline{2}]_H\}$$

dove $[\overline{0}]_H = H = [\overline{3}]_H$, $[\overline{1}]_H = \{\overline{1}, \overline{4}\} = [\overline{4}]_H$ e $[\overline{2}]_H = \{\overline{2}, \overline{5}\} = [\overline{5}]_H$.

Analogamente si ha:

$$\mathbb{Z}_6/K = \{[\overline{0}]_K, [\overline{1}]_K\}$$

dove $[\overline{0}]_K = K = [\overline{2}]_K = [\overline{4}]_K$ e $[\overline{1}]_K = \{\overline{1}, \overline{3}, \overline{5}\} = [\overline{3}]_K = [\overline{5}]_K$.

Esempio 2.2.14 Consideriamo l'insieme $Q = \{1, -1, i, -i, j, -j, k, -k\}$, su cui definiamo un'operzione binaria richiedendo che 1 sia elemento neutro e ponendo

$$i^2 = j^2 = k^2 = -1, \quad i \cdot j = -j \cdot i = k, \quad j \cdot k = -k \cdot j = i, \quad k \cdot i = -i \cdot k = j.$$

Si verifica facilmente che $(Q, \cdot)$ è un gruppo non commutativo che viene chiamato *gruppo delle unità dei quaternioni*. Tale gruppo possiede, oltre ai sottogruppi banali, i seguenti sottogruppi:

$$H = \{1, -1\},\ K_1 = \{1, -1, i, -i\},\ K_2 = \{1, -i, j, -j\},\ K_3 = \{1, -1, k, -k\}.$$

I sottogruppi K_i, $i = 1, 2, 3$, sono sicuramente normali in quanto di indice due; verifichiamo che anche H è normale e costruiamo il gruppo quoziente Q/H.

Osserviamo innanzitutto che la normalità di H è conseguenza immediata del fatto che gli elementi 1 e -1 commutano con ogni altro elemento di Q; pertanto risulta:

$$Q/H = \{H, iH, jH, kH\}, \quad iH = \{i, -i\}, \quad jH = \{j, -j\}, \quad kH = \{k, -k\}.$$

Lo studente verifichi che la tabella moltiplicativa di questo gruppo è assolutamente analoga a quella del gruppo di Klein e provi a scrivere un isomorfismo fra i due gruppi.

2.3 GRUPPI CICLICI

Vogliamo ora studiare una particolare famiglia di gruppi dei quali abbiamo già visto degli esempi, come il gruppo delle radici n-esime dell'unità.

Definizione 2.3.1 Diremo che un gruppo G è *ciclico* e $x \in G$ è un suo *generatore* se, e solo se, il sottogruppo generato da x è tutto G, ovvero $G =< x >$.

Osservazione 2.3.1 Ogni gruppo ciclico è commutativo poiché il prodotto di due potenze dello stesso elemento è ovviamente commutativo.

Esempio 2.3.1 Come esempio di gruppo ciclico infinito possiamo considerare il gruppo $(\mathbb{Z},+)$; infatti i sottogruppi generati dagli interi 1 e -1 coincidono con tutto $\mathbb{Z}$. Ogni altro intero relativo genera un sottogruppo proprio e in particolare risulta $< n >= n\mathbb{Z}= (-n)\mathbb{Z}$.

Esempio 2.3.2 Come esempio di caso finito si verifica facilmente che il gruppo $(\mathbb{Z}_m, +)$ è ciclico per ogni m; risulta infatti $o(\overline{1}) = m$ e, per $1 \leq a \leq m$, $\overline{a} = \underbrace{\overline{1} + \ldots + \overline{1}}_{a-\text{volte}}$.

Esempio 2.3.3 Abbiamo già esaminato i casi $m = 6$ e $m = 18$; vediamo ancora il caso $m = 12$ ovvero

$$\mathbb{Z}_{12} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{9}, \overline{10}, \overline{11}\}$$

Si verifica facilmente che $\overline{1}$ è un generatore del gruppo; infatti risulta:

$$\overline{1} + \overline{1} = \overline{2},\ \overline{1} + \overline{1} + \overline{1} = \overline{3},\ \ldots,\ \overline{1} + \overline{1} + \overline{1} + \overline{1} + \overline{1} + \overline{1} + \overline{1} + \overline{1} + \overline{1} + \overline{1} + \overline{1} = \overline{11}.$$

Vediamo quali sono i sottogruppi generati dagli altri elementi; ricordiamo che determinare tali sottogruppi equivale a determinare l'ordine dei diversi elementi. Otteniamo:

$$< \overline{0} >= \{\overline{0}\},\ < \overline{2} >= \{\overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12} = \overline{0}\},\ < \overline{3} >= \{\overline{3}, \overline{6}, \overline{9}, \overline{0}\},\ < \overline{4} >=$$

$$= \{\overline{4}, \overline{8}, \overline{0}\},\ < \overline{5} >= \{\overline{5}, \overline{10}, \overline{3}, \overline{8}, \overline{1}, \overline{6}, \overline{11}, \overline{4}, \overline{9}, \overline{2}, \overline{7}, \overline{0}\} =< \overline{1} >,\ < \overline{6} >= \{\overline{6}, \overline{0}\}.$$

Esaminando tutti i casi possibili lo studente trova la situazione seguente:

$$\mathbb{Z}_{12} =< \overline{1} >=< \overline{5} >=< \overline{7} >=< \overline{11} >, \quad < \overline{2} >=< \overline{10} >,$$

$$< \overline{3} >=< \overline{9} >, \quad < \overline{4} >=< \overline{8} >, \quad < \overline{6} >, \quad < \overline{0} > .$$

Denotiamo con $\varphi(k)$ il numero degli interi positivi minori di k e primi con k. Abbiamo dunque determinato un sottogruppo per ogni divisore dell'ordine, inoltre un sottogruppo di ordine k ha $\varphi(k)$ possibili generatori (ricordiamo che $\varphi(k)$ denota il numero degli interi positivi minori di k e primi con k). Inoltre nel gruppo esistono esattamente $\varphi(k)$ elementi di ordine k.

Quanto visto può essere dimostrato in generale per i gruppi ciclici finiti.

Proposizione 2.3.1 *Sia G un gruppo e $g \in G$ un elemento di ordine n. Allora*

$$o(g^k) = \frac{n}{(n,k)}.$$

Proposizione 2.3.2 *Sia G un gruppo ciclico con n elementi e sia $g \in G$ un suo generatore. Allora l'elemento g^h è un generatore di G se, e solo se, n e h sono primi fra loro, ovvero $(n,h) = 1$.*

Dimostrazione delle Proposizioni - La seconda proposizione segue dalla prima ricordando che l'ordine di un elemento coincide con la cardinalità del sottogruppo ciclico da esso generato. Pertanto basta povare che se $g \in G$ ha ordine n, allora $o(g^k) = \frac{n}{(n,k)}$. Poichè n divide $\frac{kn}{(n,k)}$, si ha

$$(g^k)^{n/(n,k)} = u.$$

Ne segue che $o(g^k)$ divide $\frac{n}{(n,k)}$. D'altra parte

$$g^{k \cdot o(g^k)} = (g^k)^{o(g^k)} = u$$

pertanto n divide $k \cdot o(g^k)$, dunque $n/(n,k)$ divide $o(g^k)$.

Possiamo ora dimostrare una caratterizzazione dei sottogruppi di un gruppo ciclico qualsivoglia.

Proposizione 2.3.3 *Ogni sottogruppo di un gruppo ciclico G è ciclico.*

Dimostrazione - Sia T un sottogruppo del gruppo G e sia g un generatore di G; se T è uno dei due sottogruppi banali non c'è nulla da dimostrare.

Sia dunque T non banale; pertanto esistono g^k e g^{-k} in T, $k \neq 0, \pm 1$. Sia ora $h \geq 2$ l'esponente minimo positivo di g per il quale risulta $g^h \in T$; vogliamo dimostrare che $T =< g^h >$, ovvero che g^h è un generatore di T. A tal fine osserviamo innanzitutto che, ovviamente, $< g^h > \subseteq T$; per dimostrare l'altra inclusione verifichiamo che ogni elemento di T è una potenza di g^h. Sia dunque $g^k \in T$, dividendo k per h si ha $k = hq + r$, $0 \leq r < h$, e pertanto $g^k = (g^h)^q g^r$; risulta allora $g^r = g^k g^{-hq} \in T$ e, per la minimalità di h, deve essere $r = 0$ ovvero $g^k = (g^h)^q$, pertanto $T =< g^h >$ è ciclico. ∎

Per i gruppi ciclici finiti è inoltre possibile dimostrare la seguente proposizione.

Proposizione 2.3.4 *Se G è un gruppo ciclico con n elementi allora per ogni d che divide n esiste un unico sottogruppo S di ordine d.*

Dimostrazione - Osserviamo innanzitutto che, se g è un generatore di G, come conseguenza di quanto dimostrato nella proposizione **??** otteniamo anche che, se $n = d \cdot t$, allora il sottogruppo $S =< g^t >$ è ciclico di ordine d.

Sia ora T un altro sottogruppo di ordine d, tale sottogruppo è ciclico per quanto visto nella proposizione precedente e quindi $T =< g^k >$ per qualche k; risulta allora:

$$d = \frac{n}{t} = o(g^k) = \frac{n}{(n,k)} \;\Rightarrow\; t = (n,k) \;\Rightarrow\; k = t \cdot s,\; s \in \mathbb{Z}.$$

Pertanto $g^k = (g^t)^s$ appartiene a S, da cui $T \subseteq S$ e, essendo S e T entrambi sottogruppi di ordine d, deve risultare $T = S$. ∎

Osservazione 2.3.2 Riassumendo quanto detto finora possiamo dire che, se G è un gruppo ciclico di ordine n e d divide n, allora G contiene esattamente $\varphi(d)$ elementi di ordine d, ciascuno dei quali è un generatore dell'unico sottogruppo di ordine d.

La funzione $\varphi(d)$ è detta *funzione di Eulero* ed è esplicitamente calcolabile a partire dalla fattorizzazione in primi di d. Risulta infatti, se $d = p_1^{h_1} \cdots p_r^{h_r}$

$$\varphi(d) = \left(p_1^{h_1} - p_1^{h_1-1}\right) \cdot \cdots \cdot \left(p_r^{h_r} - p_r^{h_r-1}\right).$$

In effetti, è chiaro che $\varphi(p) = p-1$ e non è difficile vedere che $\varphi(p^n) = p^n - p^{n-1}$. A questo punto la fornula precedente segue dal fatto che la funzione di Eulero è *moltiplicativa* se $(h,k) = 1$, cioè $\varphi(hk) = \varphi(h)\varphi(k)$.

Non tutti i gruppi sono ciclici, ad esempio un gruppo non commutativo non può essere ciclico. Un esempio di gruppo commutativo ma non ciclico è il seguente.

Esempio 2.3.4 Studiamo la struttura del gruppo degli invertibili di $\mathbb{Z}_8$:

$$\mathbb{U}(8) = \{\overline{a} : (a,8) = 1;\; \overline{a} \in \mathbb{Z}_8\} = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$$

poiché gli elementi di tale gruppo, diversi dall'unità, hanno periodo due, come lo studente può verificare, il gruppo $\mathbb{U}(8)$ possiede tre sottogruppi con due elementi e quindi non è ciclico. Si osservi come la tabella moltiplicativa di $\mathbb{U}(8)$ coincida con quella del gruppo di Klein. Con una terminologia che sarà precisata in seguito, diremo che i due gruppi sono *isomorfi*.

Alla fine del paragrafo sugli omomorfismi potremo dimostrare un teorema di caratterizzazione dei gruppi ciclici e studiare gli isomorfismi di un gruppo ciclico in se stesso.

2.4 GRUPPI DI PERMUTAZIONI

In questo paragrafo presentiamo la famiglia dei gruppi di permutazioni su un insieme finito; abbiamo già studiato la struttura del gruppo $\mathcal{S}_3$ vediamo ora cosa possiamo dire in generale.

Sia $\mathcal{S}_n$ l'insieme delle permutazioni, ovvero delle corrispondenze biunivoche, di un insieme T, con n elementi, in se stesso; esaminiamo in dettaglio la sua struttura rispetto al prodotto operatorio '$\circ$'. Sappiamo già che il prodotto operatorio è un'operazione associativa e che l'applicazione identica id_T è essa stessa una biiezione e gode della proprietà che, $\forall\ f \in \mathcal{S}_n$, $f \circ id_T = id_T \circ f = f$; inoltre è ben noto che, per ogni biiezione f, esiste la biiezione inversa f^{-1} tale che $f \circ f^{-1} = f^{-1} \circ f = id_T$. Pertanto $(\mathcal{S}_n, \circ)$ è un gruppo di ordine $n!$; tale gruppo, per $n \geq 3$, non è commutativo.

Appare evidente che la natura dell'insieme T è irrilevante ai fini dello studio della struttura del gruppo $(\mathcal{S}_n, \circ)$, pertanto nel seguito supporremo sempre $T = = \{1, 2, \ldots, n\}$ e indicheremo l'applicazione identica con id. Per semplicità di notazione utilizzeremo spesso la giustapposizione $\sigma\tau$ per indicare il prodotto operatorio $\sigma \circ \tau$; ricordiamo che, essendo σ e τ due applicazioni, il prodotto operatorio $\sigma \circ \tau$ è l'applicazione che si ottiene eseguendo prima τ e poi σ.

Definizione 2.4.1 Il gruppo $(\mathcal{S}_n, \circ)$ viene detto *gruppo simmetrico di grado* n.

Definizione 2.4.2 Si dice che la permutazione $\sigma \in \mathcal{S}_n$ *agisce in modo non banale* sull'elemento $t \in T$ se $\sigma(t) \neq t$.

Allo scopo di studiare la struttura di questo gruppo possiamo introdurre una particolare scrittura dei suoi elementi; introduciamo innanzitutto la nozione di ciclo.

Definizione 2.4.3 Una permutazione σ di $\mathcal{S}_n$ si chiama *ciclo di lunghezza* h, $h \leq n$, se essa agisce in modo non banale su ogni elemento di un sottoinsieme S di T con h elementi e risulta inoltre, per un opportuno ordinamento dell'insieme $S = = \{t_1, t_2, \ldots, t_h\}$:

$$\sigma(t_1) = t_2,\ \sigma(t_2) = t_3,\ \ldots\ , \sigma(t_h) = t_1.$$

Scriveremo allora

$$\sigma = (t_1\, t_2\, \ldots\, t_h).$$

Un ciclo di lunghezza due viene detto *trasposizione* o *scambio.*

Definizione 2.4.4 Due cicli si dicono *disgiunti* se tali sono i sottoinsiemi di T su cui essi agiscono in modo non banale.

Osservazione 2.4.1 Osserviamo che, se due cicli γ_1 e γ_2 sono disgiunti, per il loro prodotto risulta $\gamma_1 \circ \gamma_2 = \gamma_2 \circ \gamma_1$.

Esempio 2.4.1 Consideriamo le seguenti permutazioni in $\mathcal{S}_8$:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 7 & 1 & 5 & 2 & 4 & 8 \end{pmatrix},\ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 5 & 3 & 2 & 7 & 6 & 8 & 4 \end{pmatrix},$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 7 & 5 & 8 & 6 \end{pmatrix}$$

allora gli insiemi su cui operano, in modo non banale, le tre permutazioni sono rispettivamente:

$$S_1 = \{1, 2, 3, 4, 6, 7\},\ S_2 = \{2, 4, 5, 7, 8\},\ S_3 = \{1, 2, 3, 4, 5, 6, 7, 8\}.$$

Analizzando la struttura delle tre permutazioni vediamo che solamente σ_2 è un ciclo, infatti risulta:

$$\sigma_2(2) = 5,\ \sigma_2(5) = 7,\ \sigma_2(7) = 8,\ \sigma_2(8) = 4,\ \sigma_2(4) = 2$$

e scriveremo

$$\sigma_2 = (25784)(1)(3)(6) = (1)(6)(57842)(3) = (3)(78425)(6)(1) = \dots$$

Per quanto riguarda le altre due possiamo scriverle come prodotto di più cicli disgiunti e risulta:

$$\sigma_1 = (1374)(26) = (62)(3741) = (62)(8)(3741) = ...$$

e

$$\sigma_3 = (21)(34)(8657) = (6578)(12)(34) = (6578)(12)(34) = ...$$

Osserviamo che, nella fattorizzazione di σ_2, abbiamo scritto anche cicli di lunghezza uno, per semplicità di scrittura questi cicli vengono di solito omessi.

Quanto fatto nel caso particolare dell'esempio può essere ripetuto per ogni permutazione; vale infatti la seguente proposizione.

Proposizione 2.4.1 *Ogni elemento del gruppo $\mathcal{S}_n$ si scrive come prodotto di cicli disgiunti, in modo unico a meno dell'ordine.*

Dimostrazione - Sia σ una permutazione qualsiasi; preso comunque un elemento t di $T = \{1.2. \dots, n\}$ possiamo costruire un ciclo considerando le immagini successive di t fino a riottenere t stesso:

$$t,\ \sigma(t),\ \sigma^2(t), \dots \sigma^h(t),\ \sigma^{h+1}(t) = t$$

Bisogna osservare che, essendo T finito, sicuramente, dopo un numero finito di passi, dovremo ottenere un elemento già considerato precedentemente; d'altra parte, per l'iniettività di σ l'unico elemento che possiamo ottenere è proprio t.

Abbiamo quindi costruito un primo ciclo $\gamma_1 = (t\,\sigma(t)\ldots\sigma^h(t))$ di lunghezza h; se $\sigma = \gamma_1$ abbiamo finito, altrimenti prendiamo un elemento $s \in T$ su cui σ, ma non γ_1, opera in maniera non banale e ripetiamo il procedimento fino ad ottenere un ciclo γ_2 che, per l'iniettività di σ, è sicuramente disgiunto da γ_1.

Iterando il procedimento un numero finito di volte si ottiene la fattorizzazione richiesta $\sigma = \gamma_1\gamma_2\ldots\gamma_u$; l'unicità della fattorizzazione è conseguenza della costruzione stessa.

Sia infatti $\sigma = \gamma'_1\gamma'_2\ldots\gamma'_v$, allora per ogni elemento t su cui σ opera in modo non banale devono esistere esattamente un ciclo γ_i e un ciclo γ'_j che operano in modo non banale su t; in particolare deve essere:

$$\gamma_i(t) = \sigma(t) = \gamma'_j(t),\ \gamma_i^2(t) = \sigma^2(t) = (\gamma'_j)^2(t), \ldots$$

e questo implica $\gamma_i = \gamma'_j$. Pertanto le due fattorizzazioni sono, a meno dell'ordine dei fattori, la stessa fattorizzazione. ∎

Definizione 2.4.5 Nel gruppo $\mathcal{S}_n$ sia $\sigma = \gamma_1 \circ \gamma_2 \circ \ldots \circ \gamma_k$, dove i γ_i sono cicli disgiunti di lunghezza rispettivamente $1 \leq h_1 \leq h_2 \leq \ldots \leq h_k$, e ovviamente $h_1 + h_2 + \ldots + h_k = n$; allora la k-pla $(h_1, h_2, \ldots, h_k)$ viene detta *struttura ciclica* di σ.

Vediamo come la conoscenza della struttura ciclica di una permutazione ci fornisce diverse informazioni.

Proposizione 2.4.2 *L'ordine $o(\sigma)$ di un elemento del gruppo $\mathcal{S}_n$ si può calcolare al modo seguente:*

$$o(\sigma) = h \text{ se } \sigma \text{ è un ciclo di lunghezza } h,$$

$$o(\sigma) = m.c.m.(h_1, h_2, \ldots, h_k) \text{ se } \sigma \text{ ha struttura ciclica } (h_1, h_2, \ldots, h_k).$$

Dimostrazione - La prima affermazione è una ovvia conseguenza della definizione di ciclo; dimostriamo la seconda.

Sia $\sigma = \gamma_1 \circ \gamma_2 \circ \ldots \circ \gamma_k$, dove i γ_i sono cicli disgiunti di lunghezza rispettivamente h_1, h_2, ..., h_k e sia $h = m.c.m.(h_1, h_2, \ldots, h_k)$ il minimo comune multiplo delle lunghezze dei cicli; indicato con m l'ordine di σ dobbiamo dimostrare che $h = m$.

Osserviamo innanzitutto che, essendo il prodotto di cicli disgiunti commutativo, e poiché h_i divide h per ogni i, risulta:

$$\sigma^h = (\gamma_1 \circ \gamma_2 \circ \ldots \circ \gamma_k)^h = (\gamma_1)^h \circ (\gamma_2)^h \circ \ldots \circ (\gamma_k)^h = id \circ id \circ \ldots \circ id = id$$

pertanto, per le proprietà dell'ordine di un elemento, m divide h.

Dimostriamo ora che h divide m; si ha:

$$id = \sigma^m = (\gamma_1 \circ \gamma_2 \circ \ldots \circ \gamma_k)^m = (\gamma_1)^m \circ (\gamma_2)^m \circ \ldots \circ (\gamma_k)^m$$

e tale uguaglianza, essendo i cicli disgiunti, è possibile soltanto se ogni fattore del prodotto è l'identità. Se infatti fosse, ad esempio, $(\gamma_1)^m \neq id$ allora dovrebbe

essere $(\gamma_2)^h \circ \ldots \circ (\gamma_k)^h = (\gamma_1)^{-m}$ e questo è impossibile perché gli insiemi su cui agiscono, in modo non banale, i cicli sono disgiunti.

Pertanto $(\gamma_i)^m = id$, e quindi h_i divide m, $\forall\ i = 1, \ldots, k$, e, per le proprietà del minimo comune multiplo, anche h divide m. ■

Esempio 2.4.2 Determiniamo l'ordine delle seguenti permutazioni di $\mathcal{S}_7$

$$\sigma_1 = (14)(25)(376),\ \sigma_2 = (1724)(35),\ \sigma_3 = (175)(2634)$$

calcolandone le potenze successive. Si ha:

$$\sigma_1^2 = (367),\ \sigma_1^3 = (14)(25),\ \sigma_1^4 = (376),\ \sigma_1^5 = (14)(25)(367),\ \sigma_1^6 = id$$

$$\sigma_2^2 = (12)(74),\ \sigma_2^3 = (1427)(35),\ \sigma_2^4 = id$$

$$\sigma_3^2 = (157)(23)(64),\ \sigma_3^3 = (2436),\ \sigma_3^4 = (175),\ \sigma_3^5 = (157)(2634),$$

$$\sigma_3^6 = (23)(64),\ \sigma_3^7 = (175)(2436),\ \sigma_3^8 = (157),\ \sigma_3^9 = (2636),$$

$$\sigma_3^{10} = (175)(23)(64),\ \sigma_3^{11} = (157)(2436),\ \sigma_3^{12} = id$$

Pertanto risulta

$$o(\sigma_1) = 6 = m.c.m.(2,3),\ o(\sigma_2) = 4 = m.c.m.(2,4),\ o(\sigma_3) = 12 = m.c.m.(3,4);$$

osserviamo poi che $< \sigma_3 >$ è un sottogruppo ciclico con 12 elementi che possiede quattro sottogruppi non banali:

$$< \sigma_3^2 >, \quad < \sigma_3^3 >, \quad < \sigma_3^4 >, \quad < \sigma_3^6 >$$

di ordini rispettivamente 6, 4, 3 e 2.

Esempio 2.4.3 Determiniamo i possibili ordini degli elementi del gruppo $\mathcal{S}_7$; a tale scopo basta determinare tutte le possibili strutture cicliche, ovvero tutte le k-ple ordinate di interi positivi $(h_1, h_2, \ldots, h_k)$ tali che $h_1 + h_2 + \ldots + h_k = 7$.

Elenchiamo le strutture cicliche e, per ciascuna diamo un esempio, risulta allora:

struttura ciclica	σ	$o(\sigma)$
$1+1+1+1+1+1+1$	id	1
$1+1+1+1+1+2$	(12)	2
$1+1+1+1+3$	(123)	3
$1+1+1+4$	(1234)	4
$1+1+5$	(12345)	5
$1+6$	(123456)	6
7	(1234567)	7
$1+1+1+2+2$	(12)(34)	2
$1+1+2+3$	(12)(345)	6
$1+2+4$	(12)(3456)	4
$2+5$	(12)(34567)	10
$1+2+2+2$	(12)(34)(56)	2
$2+2+3$	(12)(34)(567)	6
$1+3+3$	(123)(456)	3
$3+4$	(123)(4567)	12

Per una permutazione decomposta in cicli disgiunti è immediato scrivere la permutazione inversa.

Proposizione 2.4.3 *Se σ è un ciclo, $\sigma = (t_1\, t_2\, \ldots\, t_h)$, allora*

$$\sigma^{-1} = (t_h\, t_{h-1}\, \ldots\, t_1)$$

Se $\sigma = \gamma_1 \circ \gamma_2 \circ \ldots \circ \gamma_k$, è prodotto di cicli disgiunti allora

$$\sigma^{-1} = \gamma_1^{-1} \circ \gamma_2^{-1} \circ \ldots \circ \gamma_k^{-1}$$

Dimostrazione - La prima affermazione è una immediata conseguenza della definizione di ciclo; la seconda affermazione segue dalla proposizione **??** e dal fatto che il prodotto di cicli disgiunti è commutativo. ∎

Esempio 2.4.4 Per calcolare l'inversa della permutazione su 8 elementi:

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

possiamo sia 'scambiare' la seconda riga con la prima e riordinare al modo seguente:

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

oppure scrivere σ come prodotto di cicli disgiunti e applicare la proposizione precedente:

$$\sigma = (1856)(247) \implies \sigma^{-1} = (1658)(274).$$

Vediamo ora una proprietà importante delle permutazioni; iniziamo con l'osservare che, dato un ciclo $\gamma = (t_1\, t_2\, \ldots\, t_m)$ di lunghezza m, esso si può scrivere, in molti modi, come prodotto di $m-1$ cicli di lunghezza due, ad esempio:

$$\gamma = (t_1\, t_2\, \ldots\, t_m) = (t_1\, t_m)(t_1\, t_{m-1}) \ldots (t_1\, t_2),$$

dove i cicli di lunghezza due non sono ovviamente disgiunti.

Come conseguenza di questa osservazione abbiamo che, data una permutazione σ con struttura ciclica $(h_1, h_2, \ldots, h_s)$, tale permutazione si può scrivere, in maniera non unica, come prodotto di $\sum_{i=1}^{s}(h_i - 1)$ trasposizioni; risulta infatti:

$$\sigma = \gamma_1\gamma_2 \ldots \gamma_s = (t_{11}\, t_{12}\, \ldots\, t_{1h_1})(t_{21}\, t_{22}\, \ldots\, t_{2h_2}) \ldots (t_{s1}\, t_{s2}\, \ldots\, t_{sh_s}) =$$

$$= (t_{11}\, t_{1h_1})(t_{11}\, t_{1(h_1-1)}) \ldots (t_{11}\, t_{12})(t_{21}\, t_{2h_2})(t_{21}\, t_{2(h_2-1)}) \ldots (t_{21}\, t_{22}) \ldots$$

$$\ldots (t_{s1}\, t_{sh_s})(t_{s1}\, t_{s(h_s-1)}) \ldots (t_{s1}\, t_{s2}).$$

Esempio 2.4.5 Scriviamo la permutazione

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

di $\mathcal{S}_9$ come prodotto di cicli disgiunti (in modo unico) e poi come prodotto di cicli di lunghezza due; risulta:

$$\sigma = (1574)(392)(68) = (14)(17)(15)(32)(39)(68) =$$

$$= (75)(71)(74)(93)(92)(68) = \ldots$$

dove la decomposizione in cicli di lunghezza due cambia a seconda di come si rappresenta il ciclo di partenza.

Possiamo però fare anche altri calcoli e ottenere altre decomposizioni di σ, ad esempio:

$$\sigma = (1574)(392)(68) = (1574)(34)(34)(392)(68) =$$

$$= (15743)(2439)(68) = (51)(53)(54)(57)(34)(32)(39)(68)$$

oppure

$$\sigma = (1574)(392)(68) = (1574)(392)(56)(56)(68) =$$

$$= (392)(56741)(685) = (32)(39)(51)(54)(57)(56)(65)(68).$$

Abbiamo quindi ottenuto diverse decomposizioni tutte però in un numero pari di trasposizioni; dimostreremo che questo fatto è del tutto generale. Diamo innanzitutto una definizione che, a questo punto, appare spontanea.

Definizione 2.4.6 Siano σ una permutazione e $(h_1, h_2, \ldots, h_s)$ la sua struttura ciclica, possiamo allora definire il seguente numero:

$$N(\sigma) = \sum_{i=1}^{s} (h_i - 1).$$

Osserviamo che $N(id) = 0$ e che $N((ab)) = 1$ per ogni trasposizione (ab); possiamo a questo punto enunciare la seguente proposizione:

Proposizione 2.4.4 *Data una permutazione σ ed una sua qualsiasi decomposizione in prodotto di k trasposizioni, risulta che k è pari o dispari a seconda che $N(\sigma)$ sia pari o dispari.*

A questo punto possiamo affermare che la parità del numero $N(\sigma)$ non dipende dalla particolare decomposizione in trasposizioni; ha quindi senso la seguente definizione.

Definizione 2.4.7 Si dice che la permutazione σ è *di classe pari (dispari)* ovvero è *pari (dispari)* se $N(\sigma)$ è pari (dispari).

Osservazione 2.4.2 Il concetto di parità viene utilizzato in diverse circostanze; ad esempio ricordiamo che, se $M = (a_{ij})$, $i, j \in \{1, 2, \ldots, n\}$, è una matrice quadrata, il suo determinante può essere calcolato al modo seguente:

$$\det M = \sum_{\sigma \in \mathcal{S}_n} (-1)^{sg(\sigma)} \prod_{i=1}^{n} a_{i\sigma(i)}$$

dove $sg(\sigma) = 1$ se σ è di classe pari e $sg(\sigma) = -1$ se σ è di classe dispari.

Per il prodotto di permutazioni vale la seguente proprietà:

Proposizione 2.4.5 *Il prodotto di due permutazioni pari o di due permutazioni dispari è pari mentre il prodotto di una permutazione pari per una permutazione dispari è dispari.*

Dimostrazione - La dimostrazione è immediata quando si consideri che, moltiplicare due permutazioni decomposte rispettivamente in k_1 e k_2 trasposizioni, fornisce una permutazione decomposta in $k_1 + k_2$ trasposizioni. ∎

Corollario 2.4.1 *L'insieme $\mathcal{A}_n$ delle permutazioni di classe pari è equipotente all'insieme delle permutazioni di classe dispari, onde $|\mathcal{A}_n| = \dfrac{n!}{2}$.*

Dimostrazione - Fissata una qualsiati trasposizione τ, basta considerare la seguente applicazione:

$$\begin{array}{rccc} \psi & : & \mathcal{A}_n & \longrightarrow & \mathcal{S}_n \backslash \mathcal{A}_n \\ & & \sigma & \longrightarrow & \sigma\tau \end{array}$$

e verificare che essa è biunivoca.

Osserviamo che, se $\sigma_1\tau = \sigma_2\tau$ allora ovviamente $\sigma_1 = \sigma_2$, ovvero ψ è iniettiva; inoltre, $\forall\ \tilde{\sigma}$ dispari, $\tilde{\sigma}\tau$ è pari e risulta $\tilde{\sigma} = \psi(\tilde{\sigma}\tau)$, onde ψ è suriettiva. ∎

Proposizione 2.4.6 *L'insieme $\mathcal{A}_n$ è un sottogruppo normale del gruppo $\mathcal{S}_n$. Tale sottogruppo prende il nome di gruppo alterno su n elementi.*

Dimostrazione - Abbiamo già osservato che l'identità è pari e che il prodotto di due permutazioni pari è ancora una permutazione pari; inoltre è ovvio che $N(\sigma) = N(\sigma^{-1})$ qualunque sia σ e pertanto il fatto che $\mathcal{A}_n$ sia un sottogruppo è ovvio.

Per quanto riguarda la normalità basta osservare che, essendo $|\mathcal{A}_n| = \frac{n!}{2}$ il sottogruppo ha indice due e pertanto è normale. ∎

2.5 OMOMORFISMI FRA GRUPPI

Definizione 2.5.1 Definiamo *omomorfismo* o *morfismo* fra due gruppi $(G, \cdot)$ e $(K, *)$ un'applicazione $f : G \to K$ tale che:

$$\forall\, g, h \in G \quad \Longrightarrow \quad f(g \cdot h) = f(g) * f(h).$$

Se f è iniettiva parleremo di *monomorfismo*, se è suriettiva di *epimorfismo* ed infine se è biunivoca di *isomorfismo*.

Proposizione 2.5.1 *Se $(G, \cdot)$ e $(K, *)$ sono gruppi e $f : G \to K$ è un isomorfismo allora $f^{-1} : K \to G$ è un isomorfismo.*

Dimostrazione - Dobbiamo dimostrare che, $\forall\, x, y \in K$ risulta:

$$f^{-1}(x * y) = f^{-1}(g) \cdot f^{-1}(h);$$

a tal fine osserviamo che:

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

e, essendo f un morfismo,

$$f(f^{-1}(x) \cdot f^{-1}(y)) = f(f^{-1}(x)) * f(f^{-1}(y)) = (f \circ f^{-1})(x) * (f \circ f^{-1})(y) = x * y.$$

La tesi segue allora dal fatto che f è iniettiva. ∎

Definizione 2.5.2 Se, dati due gruppi $(G, \cdot)$ e $(K, *)$, esiste un isomorfismo $\varphi : G \to K$, diremo che i due gruppi sono *isomorfi* e scriveremo $G \cong K$.

Definizione 2.5.3 Nel caso particolare di un omomorfismo di un gruppo in se stesso parleremo di *endomorfismo* e, nel caso di un isomorfismo di un gruppo in se stesso, di *automorfismo*.

Esempio 2.5.1 L'applicazione definita per un intero qualsiasi m:

$$\begin{array}{rccc} f & : & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & & z & \longrightarrow & mz \end{array}$$

è un endomorfismo del gruppo additivo $(\mathbb{Z}, +)$; risulta infatti, $\forall\ x, y \in \mathbb{Z}$:

$$f(x+y) = m(x+y) = mx + my = f(x) + f(y).$$

Tale endomorfismo è iniettivo se $m \neq 0$ ed è suriettivo soltanto per $m = \pm 1$; risulta infatti $Imf = m\mathbb{Z}$.

Sia $(G, \cdot)$ un gruppo e N un suo sottogruppo normale; abbiamo dimostrato che l'insieme G/N delle classi laterali (sia destre che sinistre) di N, relativamente al prodotto fra classi, è esso stesso un gruppo. Considerata allora la proiezione canonica

$$\begin{array}{rccc} \pi & : & G & \longrightarrow & G/N \\ & & g & \longrightarrow & \pi(g) = gN \end{array}$$

possiamo allora osservare che, per come è definita l'operazione in G/N, per ogni g e h in G, risulta $\pi(gh) = ghN = gN \cdot hN = \pi(g) \cdot \pi(h)$.

Da quanto detto finora appare chiaro che la proiezione canonica di dominio un gruppo G e codominio un suo quoziente G/N, $N \lhd G$, è un epimorfismo di gruppi. Vediamo qualche altro esempio di omomorfismo.

Esempio 2.5.2 L'applicazione $f : (\mathbb{Z}, +) \to (\mathcal{S}_3, \circ)$ tale che $f(2k) = id$ e $f(2k+1) = \begin{pmatrix} 123 \\ 132 \end{pmatrix}$ è un omomorfismo. Infatti, $\forall\ z, w \in \mathbb{Z}$, possono verificarsi tre possibilità, z e w sono entrambi pari, entrambi dispari ovvero uno pari ed uno dispari; siano ad esempio $z = 2k+1$ e $w = 2h+1$ allora risulta:

$$f(z+w) = f(2(h+k+1)) = id$$

e

$$f(z) \circ f(w) = \begin{pmatrix} 123 \\ 132 \end{pmatrix} \circ \begin{pmatrix} 123 \\ 132 \end{pmatrix} = id$$

onde $f(z+w) = f(z) \circ f(w)$.

Gli altri due casi si verificano immediatamente alla stessa maniera.

Esempio 2.5.3 Consideriamo i seguenti gruppi $G = (\mathbb{R}, +)$ e $K = (\mathbb{R}^+, \cdot)$, ovvero il gruppo additivo dei reali e il gruppo moltiplicativo dei reali positivi.

Possiamo allora definire l'applicazione $f : \mathbb{R} \longrightarrow \mathbb{R}^+$ tale che $f(x) = a^x$, dove a è un reale positivo diverso da uno; per quanto noto dall'analisi, tale applicazione f è biunivoca ed è un omomorfismo, risulta infatti:

$$\forall\ x, y \in \mathbb{R} \quad : \quad f(x+y) = a^{x+y} = a^x \cdot a^y = f(x) \cdot f(y).$$

Otteniamo quindi che i gruppi G e K sono isomorfi.

Lo studente determini l'isomorfismo inverso dell'isomorfismo f.

Per gli omomorfismi vale la seguente proposizione:

Proposizione 2.5.2 *Siano $(G,\cdot)$ e $(K,*)$ due gruppi, $f: G \to K$ un omomorfismo, u ed e rispettivamente gli elementi neutri di G e K; allora risulta:*

1. $f(u) = e$,

2. $\forall\ g \in G$, *si ha che* $f(g)^{-1} = f(g^{-1})$,

3. $\forall\ g \in G$, *se* $o(g) = n$ *allora* $o(f(g))$ *divide* n,

4. *se f è un isomorfismo allora,* $\forall\ g \in G$, *se* $o(g)=n$ *risulta* $o(f(g)) = n$.

Dimostrazione - Per dimostrare la 1) basta osservare che risulta $f(u) = f(u\cdot u) =$ $= f(u) * f(u)$ da cui, moltiplicando per $f(u)^{-1}$, si ottiene $f(u) * f(u)^{-1} = f(u)$ e quindi $f(u) = e$.

Per quanto riguarda la 2) osserviamo che:

$$f(g) * f(g^{-1}) = f(g \cdot g^{-1}) = f(u) = e$$

onde, per l'unicità dell'inverso, $f(g^{-1}) = f(g)^{-1}$.

La 3) segue dal fatto che, se $o(g) = n$, allora $e = f(u) = f(g^n) = f(g)^n$ e dalla proposizione **??**; la 4) segue dalla 3) applicata a f e a f^{-1}. ∎

Come prima conseguenza della proposizione precedente possiamo osservare che, se G è un gruppo costituito da due elementi, allora G è isomorfo a $(\mathbb{Z}_2, +)$; infatti, essendo G un gruppo, uno dei due elementi deve essere l'elemento neutro e l'altro coincide con il proprio inverso, onde $G = \{u, a : a^2 = u\}$. L'applicazione $f : \mathbb{Z}_2 \to G$ così definita $f(\overline{0}) = u$, $f(\overline{1}) = a$ è ovviamente un isomorfismo.

Introduciamo ora un sottoinsieme di fondamentale importanza.

Definizione 2.5.4 Siano $(G,\cdot)$ e $(K,*)$ due gruppi, e l'elemento neutro di K e $f: G \to K$ un omomorfismo; si definisce *nucleo di* f il seguente sottoinsieme di G:

$$Kerf = \{g \in G\ :\ f(g) = e\}.$$

Allora è possibile dimostrare che:

Proposizione 2.5.3 *Il nucleo $Kerf$ di un omomorfismo f di dominio un gruppo G è un sottogruppo normale di G.*

Dimostrazione - Verifichiamo innanzitutto che $Kerf$ è un sottogruppo di G applicando la condizione necessaria e sufficiente per i sottogruppi; a tal fine osserviamo che $Kerf \neq \emptyset$ poiché, se u è l'elemento neutro di G, si ha $u \in Kerf$, essendo $f(u) = e$.

Risulta poi, $\forall\ g, h \in Kerf$:

$$f(g^{-1}h) = f(g^{-1}) * f(h) = f(g)^{-1} * f(h) = e^{-1} * e = e$$

onde $g^{-1}h \in Kerf$; da ciò segue che $Kerf$ è un sottogruppo di G.

Per verificare che $Kerf$ è normale basta dimostrare, cfr proposizione **??**, che xwx^{-1} appartiene a $Kerf$, $\forall\ x \in G$ e $\forall\ w \in Kerf$.

Risulta infatti

$$f(xwx^{-1}) = f(x)f(w)f(x^{-1}) = f(x)ef(x)^{-1} = e$$

e pertanto $xwx^{-1} \in Kerf$. ∎

Data una funzione è sempre definita la sua immagine; per l'immagine di un omomorfismo vale la seguente proposizione.

Proposizione 2.5.4 *Se f è un omomorfismo di codominio K allora il sottoinsieme Imf è un sottogruppo di K.*

Dimostrazione - Innanzitutto $Imf \neq \emptyset$ poiché $e \in Imf$ essendo $f(u) = e$; siano poi $h, k \in Imf$, onde esistono $x, y \in G$ tali che $f(x) = h$ e $f(y) = k$ e quindi:

$$h^{-1} * k = f(x)^{-1} * f(y) = f(x^{-1}) * f(y) = f(x^{-1} \cdot y)$$

da ciò segue che $h^{-1} * k$ appartiene ad Imf che risulta quindi essere un sottogruppo di K. ∎

Osservazione 2.5.1 L'applicazione f risulta essere un epimorfismo se, e solo se, $Imf = K$.

Per quanto riguarda il nucleo di un omomorfismo vale la seguente proposizione:

Proposizione 2.5.5 *Siano $(G, \cdot)$ e $(K, *)$ due gruppi con elementi neutri rispettivamente u ed e; sia poi f un omomorfismo del gruppo G nel gruppo K. Si ha allora che due elementi di G hanno la stessa immagine in f se, e solo se, appartengono alla stessa classe laterale modulo il nucleo.*

Dimostrazione - Presi comunque due elementi x e y in G, essendo f un omomorfismo, se $f(x) = f(y)$ allora $f(x^{-1}y) = e$ ovvero $x^{-1}y \in Kerf$; tale condizione equivale a $y \in xKerf$, ovvero x e y appartengono alla stessa classe laterale. ∎

Corollario 2.5.1 *L'applicazione f è un monomorfismo se, e solo se, il nucleo è ridotto al solo elemento neutro, ovvero $Kerf = \{u\}$.*

Osservazione 2.5.2 A questo punto possiamo osservare che la relazione di equivalenza associata alla funzione f coincide con la relazione associata alla partizione in classi laterali.

Da quanto detto finora segue che le classi laterali del nucleo di f sono le classi di equivalenza della relazione ρ tale che $x\rho y \Leftrightarrow f(x) = f(y)$, e quindi risulta $G/Kerf = G/\rho$.

Nell'ottica dell'osservazione precedente ricordiamo che la possibilità di definire le operazioni di addizione e di moltiplicazione in $\mathbb{Z}_n$ dipendeva dalla seguente proprietà della congruenza modulo n:

$$\forall\, a,b,c,d \in \mathbb{Z} \quad : \quad \left.\begin{array}{c} a \equiv c \bmod n \\ b \equiv d \bmod n \end{array}\right\} \implies \left\{\begin{array}{c} a+b \equiv c+d \bmod n \\ ab \equiv cd \bmod n \end{array}\right.$$

Vediamo che una cosa analoga succede anche per la relazione indotta in un gruppo G da un omomorfismo di dominio G.

Proposizione 2.5.6 *Se f è un omomorfismo di dominio un gruppo G allora la relazione ρ indotta da f, ovvero $g\rho h \Leftrightarrow f(g) = f(h)$, $\forall$ g e h in G, gode della seguente proprietà:*

$$g\rho h \text{ e } g'\rho h' \Longrightarrow gg'\rho hh' \ .$$

Dimostrazione - Risulta infatti:

$$f(g) = f(h) \text{ e } f(g') = f(h') \Longrightarrow f(gg') = f(g)f(g') = f(h)f(h') = f(hh') \ . \blacksquare$$

Osservazione 2.5.3 La proposizione precedente è completamente in armonia con la proposizione **??**.

Dimostriamo adesso il seguente importante teorema.

Proposizione 2.5.7 (Teorema di omomorfismo) *Se $(G,\cdot)$ e $(K,*)$ sono due gruppi e $f : G \to K$ è un omomorfismo, esiste un unico isomorfismo $\overline{f} : G/Kerf \to Imf$ tale che, $\forall$ $x \in G$, risulti $(\overline{f} \circ \pi)(x) = f(x)$.*

Dimostrazione - Definiamo $\overline{f} : G/Kerf \to Imf$ ponendo $\overline{f}([x]) = f(x)$; dobbiamo dimostrare che $\overline{f}$ è ben posta, iniettiva, suriettiva ed è un omomorfismo. Supponiamo che $[x] = [y]$: allora $xy^{-1} \in Ker\, f$, pertanto $x = ky$ per qualche $k \in Ker\, f$. Ne segue, tenendo conto che f è un omomorfismo

$$f(x) = f(ky) = f(k)\, f(y) = f(y).$$

Pertanto $\overline{f}$ è ben posta. È inoltre chiaramente suriettiva: dato $z \in Im\, f$, risulta $z = f(x)$ per qualche $x \in G$, dunque $z = f(x) = \overline{f}([x])$. Per quanto riguarda l'iniettività, supponiamo $\overline{f}([x]) = \overline{f}([y])$: allora $f(x) = f(y)$ e $f(xy^{-1}) = 1$. Dunque $xy^{-1} \in Ker\, f$, ovvero $[x] = [y]$. Resta da vedere solamente che $\overline{f}$ è un omomorfismo.

Siano dunque $xKerf$ e $yKerf$ due elementi di $G/Kerf$; risulta allora:

$$\overline{f}(xKerf \cdot yKerf) = \overline{f}(xyKerf) =$$

$$= f(xy) = f(x) * f(y) = \overline{f}(xKerf) * \overline{f}(yKerf). \blacksquare$$

Esempio 2.5.4 Consideriamo l'applicazione $f : (\mathcal{S}_n, \circ) \to (\mathbb{Z}_2, +)$ tale che $f(\sigma) = \overline{0}$, se σ è pari, e $f(\sigma) = \overline{1}$ se σ è dispari; si verifica facilmente che f è un omomorfismo. Infatti, $\forall\ \sigma, \tau \in \mathcal{S}_n$, possono verificarsi tre possibilità, σ e τ sono entrambi pari, entrambi dispari ovvero una pari ed una dispari; nel primo caso il prodotto $\sigma \circ \tau$ è pari e risulta:

$$f(\sigma \circ \tau) = \overline{0} = \overline{0} + \overline{0} = f(\sigma) + f(\tau)$$

gli altri due casi si verificano in maniera del tutto analoga.

Il nucleo dell'omomorfismo f risulta essere $Kerf = \mathcal{A}_n$; inoltre f è ovviamente suriettiva e pertanto, applicando il teorema di omomorfismo, si ottiene:

$$\mathcal{S}_n/\mathcal{A}_n \cong \mathbb{Z}_2.$$

Come applicazione del teorema di omomorfismo dimostriamo un teorema di caratterizzazione dei gruppi ciclici.

Proposizione 2.5.8 *Se G è un gruppo ciclico finito di ordine n esso è isomorfo al gruppo $(\mathbb{Z}_n, +)$; se invece G non è finito allora esso è isomorfo al gruppo $(\mathbb{Z}, +)$.*

Dimostrazione - Sia $G =< g >$ un gruppo ciclico; possiamo allora definire un'applicazione di dominio il gruppo $(\mathbb{Z},+)$ e codominio G al modo seguente:

$$\begin{array}{rccc} \alpha & : & \mathbb{Z} & \longrightarrow & G \\ & & z & \longrightarrow & g^z \end{array}$$

Tale applicazione è un omomorfismo poiché risulta, per ogni $z, w \in \mathbb{Z}$:

$$\alpha(z + w) = g^{z+w} = g^z \cdot g^w = \alpha(z) \cdot \alpha(w);$$

tale omomorfismo è suriettivo in quanto ogni elemento di G è una potenza di g.

Applicando il teorema di omomorfismo abbiamo allora che il gruppo G deve essere isomorfo al gruppo quoziente $\mathbb{Z}/Ker\alpha$, dove $Ker\alpha$ è un sottogruppo normale di $\mathbb{Z}$; abbiamo però dimostrato che i sottogruppi di $\mathbb{Z}$ sono tutti e soli del tipo $m\mathbb{Z}$ e pertanto risulterà:

$$G \cong \mathbb{Z}_m, \quad m = |G|, \quad \text{se } \alpha \text{ non è iniettiva,}$$

$$G \cong \mathbb{Z}, \text{ se } \alpha \text{ è iniettiva. } \blacksquare$$

Osserviamo che nel teorema di omomorfismo, l'omomorfismo f viene decomposto nel prodotto di due omomorfismi. In generale sussiste la seguente proposizione.

Esercizio 4 *Siano $(G, \cdot)$, $(K, *)$ e $(H, \star)$ tre gruppi e $f : G \to K$ e $g : K \to H$ due omomorfismi; allora il prodotto operatorio $g \circ f : G \to H$ è un omomorfismo.*

Dimostrazione - Osserviamo che, $\forall\ x, y \in G$, risulta

$$(g \circ f)(x \cdot y) = g(f(x \cdot y)) = g(f(x) * f(y)) =$$

$$= g(f(x)) \star g(f(y)) = (g \circ f)(x) \star (g \circ f)(y)$$

onde $g \circ f$ è un omomorfismo. ∎

Quanto appena affermato ci permette di dimostrare il seguente risultato:

Esercizio 5 *Siano $(G, \cdot)$ un gruppo e $Aut(G) = \{\alpha : G \leftrightarrow G\}$ l'insieme di tutti gli automorfismi di G; allora $(Aut(G), \circ)$ è un gruppo.*

Dimostrazione - Sappiamo già che il prodotto operatorio è un'operazione associativa; inoltre l'applicazione identica è ovviamente un isomorfismo.

Infine la proposizione **??** ci assicura che, $\forall\ g, h \in G$:

$$\alpha^{-1}(g \cdot h) = \alpha^{-1}(g) \cdot \alpha^{-1}(h);$$

ovvero che α^{-1} è un isomorfismo. ∎

Fra gli automorfismi di un gruppo ne esiste una famiglia che riveste una grande importanza, quella degli automorfismi interni; diamone la definizione e vediamo alcuni esempi.

Proposizione 2.5.9 *Sia G un gruppo e $g \in G$; allora l'applicazione γ_g di dominio e codominio il gruppo G, definita al modo seguente:*

$$\forall\ x \in G\ : \gamma_g(x) = gxg^{-1}$$

è un automorfismo.

Dimostrazione - L'applicazione è iniettiva, infatti:

$$\gamma_g(x) = \gamma_g(y)\ \Longrightarrow\ gxg^{-1} = gyg^{-1}\ \Longrightarrow\ x = y$$

per quanto riguarda la suriettività si ha:

$$\forall\ z \in G\ : \gamma_g(g^{-1}zg) = z$$

infine l'applicazione verifica la condizione di omomorfismo infatti:

$$\forall\ x, y \in G\ : \gamma_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \gamma_g(x)\gamma_g(y).$$ ∎

Definizione 2.5.5 L'applicazione γ_g di cui alla proposizione precedente viene detta *automorfismo interno.*

Proposizione 2.5.10 *L'insieme $Int(G) = \{\gamma_g : g \in G\}$ è un sottogruppo normale del gruppo $Aut(G)$ di tutti gli automorfismi di G.*

Dimostrazione - Verifichiamo innanzitutto che il prodotto di due automorfismi interni è un automorfismo interno; infatti:

$$\forall\ \gamma_g, \gamma_h \in Int(G) \text{ e } \forall\ x \in G\ :\ (\gamma_g \circ \gamma_h)(x) = \gamma_g(\gamma_h(x)) =$$

$$= \gamma_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = \gamma_{gh}(x).$$

Pertanto $\gamma_g \circ \gamma_h = \gamma_{gh}$ e quindi $id = \gamma_u$ e $\gamma_g^{-1} = \gamma_{g^{-1}}$ e quindi $Int(G)$ è un sottogruppo di $Aut(G)$.

Per dimostrare che $Int(G)$ è un sottogruppo normale di $Aut(G)$ verifichiamo che, $\forall\ \alpha \in Aut(G)$ e $\forall\ \gamma_g \in Int(G)$, risulta $\alpha \circ \gamma_g \circ \alpha^{-1} \in Int(G)$.

Se x è l'elemento generico di G abbiamo le seguenti uguaglianze:

$$(\alpha \circ \gamma_g \circ \alpha^{-1})(x) = (\alpha \circ \gamma_g)(\alpha^{-1}(x)) = \alpha(\gamma_g(\alpha^{-1}(x))) = \alpha(g \cdot \alpha^{-1}(x) \cdot g^{-1}) =$$

$$= \alpha(g) \cdot \alpha(\alpha^{-1}(x)) \cdot \alpha(g^{-1}) = \alpha(g) \cdot x \cdot \alpha(g)^{-1} = \gamma_{\alpha(g)}(x)$$

e pertanto risulta:

$$\alpha \circ \gamma_g \circ \alpha^{-1} = \gamma_{\alpha(g)}$$

e la proposizione è dimostrata. ■