Capitolo 6

Ancora sui gruppi: sottogruppi e omomorfismi

Da ora in poi, nella trattazione generale useremo sempre (salvo diverso avviso esplicito) la notazione moltiplicativa per i gruppi.

§ 6.1 Sottogruppi di un gruppo

Definizione 6.1. *Siano $(G, \cdot)$ un gruppo e H un sottoinsieme di G. Si dice che H è un* **sottogruppo** *di G e si scrive $H < G$ se H è un gruppo con l'operazione indotta da quella di G. Più esplicitamente, H è un sottogruppo di G se*

- $1_G \in H$
- $\forall a, b \in H$, *si ha* $a \cdot b \in H$
- $\forall a \in H$, *si ha* $a^{-1} \in H$.

Spesso per verificare se un sottoinsieme di un gruppo è un suo sottogruppo è comodo utilizzare il seguente

Proposizione 6.2 (Criterio dei sottogruppi)**.** *Un sottoinsieme H di un gruppo $(G, \cdot)$ è un suo sottogruppo se e solo se soddisfa la seguente condizione:*

$$H \neq \emptyset \quad e \quad \forall a, b \in H \quad si\ ha \quad a \cdot b^{-1} \in H.$$

Dimostrazione. Supponiamo che H sia un sottogruppo di G. Poichè $1_G \in H$, allora $H \neq \emptyset$. Se inoltre $a, b \in H$, allora per definizione di sottogruppo anche $b^{-1} \in H$ e quindi $ab^{-1} \in H$. Quindi il sottogruppo H soddisfa il criterio. Supponiamo viceversa che H sia un sottoinsieme di G che soddisfa il criterio. Proviamo che soddisfa anche le tre condizioni per essere un sottogruppo. Prendiamo un qualsiasi elemento $a \in H$ (che esiste perché $H \neq \emptyset$), allora per il criterio $1_G = a \cdot a^{-1} \in H$. Applicando poi la condizione data dal criterio ai due elementi 1_H e a otteniamo $a^{-1} = 1_G \cdot a^{-1} \in H$. Se infine $a, b \in H$, per quanto abbiamo già provato sappiamo che $b^{-1} \in H$. Applicando il criterio alla coppia $a, b^{-1} \in H$, otteniamo $a \cdot b = a \cdot (b^{-1})^{-1} \in H$. □

Esempio 6.3. Il sottoinsieme $\mathbb{Z}$ di $\mathbb{Q}$ è un sottogruppo del gruppo $(\mathbb{Q}, +)$. Infatti $\mathbb{Z} \neq \emptyset$ e per ogni $x, y \in \mathbb{Z}$ la somma tra x e l'opposto di y sta in $\mathbb{Z}$. Invece $\mathbb{N}$ non è un sottogruppo di $(\mathbb{Q}, +)$. Infatti, $3, 7 \in \mathbb{N}$, ma $3 + (-7) \notin \mathbb{N}$.

Esempio 6.4. Il sottoinsieme $\mathbb{Q}_+$ dei numeri razionali positivi è un sottogruppo di $(\mathbb{Q} \setminus \{0\}, \cdot)$. Infatti l'identità 1 del gruppo appartiene a $\mathbb{Q}_+$, l'inverso di un numero razionale positivo è un numero razionale positivo e il prodotto di due numeri razionali positivi è ancora un numero razionale positivo. Invece $\mathbb{Q}_-$ dei razionali negativi non è un sottogruppo.

Esempio 6.5. Il sottoinsieme delle permutazioni pari di S_n è un sottogruppo di S_n. Infatti la permutazione identità è pari, componendo due permutazioni pari si ottiene una permutazione pari e l'inversa di una permutazione pari è pari. Questo sottogruppo si chiama **gruppo alterno** su n elementi e si denota A_n. Invece le permutazioni dispari di S_n non formano un suo sottogruppo, poiché ad esempio non contiene la funzione identità .

Esempio 6.6. Il sottoinsieme $5\mathbb{Z}$ dei multipli interi di 5 è un sottogruppo del gruppo $(\mathbb{Z}, +)$. Infatti $5\mathbb{Z} \neq \emptyset$ e la differenza tra due multipli interi di 5 è un multiplo intero di 5.

§ 6.2 Quanti elementi ha un sottogruppo: il Teorema di Lagrange

Fissiamo ora un gruppo $(G, \cdot)$, un suo sottgruppo H e un suo elemento g. L'insieme $\{gh \mid h \in H\}$ si denota con gH e si dice **laterale sinistro di H rappresentato da g**; in modo analogo potremmo definire il laterale destro.

Proposizione 6.7. *Con le notazioni precedenti:*

i) $|H| = |gH|$.

ii) $gH = g'H \iff g^{-1}g' \in H$.

iii) I laterali sinistri formano una partizione di G.

Dimostrazione. i) La funzione $\mu_g \colon H \to gH$ data da $\mu_g(h) = gh$ è biunivoca poiché ha come inversa la funzione $gH \to H$ che moltiplica ogni elemento gh a sinistra per g^{-1}. ii) "$\Longrightarrow$" Poiché $g' = g' \cdot 1_G \in g'H = gH$, allora esiste $h \in H$ tale che $g' = gh$ e quindi $g^{-1}g' = h \in H$. "$\Longleftarrow$" Sia $a := (g^{-1}g')^{-1} \in H$ e sia gk, un qualsiasi elemento di gH. Allora $gk = g(g^{-1}g'a)k = (gg^{-1})g'(ak) = g'(ak) \in g'H$. Di conseguenza $gH \subset g'H$. Per motivi di simmetria vale anche l'altra inclusione e quindi $gH = g'H$. iii) Nessun laterale gH è vuoto, poiché $1_G \in H$ e quindi $g = g \cdot 1_H \in gH$. Per lo

stesso motivo l'unione dei laterali è tutto G. Due laterali sinistri gH e $g'H$ hanno un elemento a in comune se e solo se esistono $h, m \in H$ tali che $a = gh = g'm$. Allora $g^{-1}g' = hm^{-1} \in H$ e quindi, grazie a ii), concludiamo che $gH = g'H$. □

Corollario 6.8 (Teorema di Lagrange)**.** *Se G è un gruppo finito ed H è un suo sottogruppo, allora il numero di elementi di H divide esattamente il numero di elementi di G.*

Dimostrazione. Abbiamo dimostrato che i laterali sinistri di H formano una partizione di G e che inoltre ciascuno di essi ha lo stesso numero di elementi di H. Dunque possiamo ottenere il numero di elementi di G moltiplicando il numero di elementi di H per il numero di laterali sinistri diversi. □

Esempio 6.9 (Il gruppo alterno)**.** è facile verificare che il sottoinsieme A_n delle permutazioni pari di S_n è un suo sottogruppo (detto **gruppo alterno**). Ogni laterale sinistro σA_n costituito da permutazioni con la stessa parità del rappresentante σ. Poiché la composizione di due permutazioni pari è pari e la composizione di due permutazioni dispari è pari, vi saranno due soli laterali A_n stesso e l'insieme formato dalle permutazioni dispari. Quindi il numero di elementi di A_n è $\frac{n!}{2}$.

Esempio 6.10. Il sottogruppo S_4 ha 24 elementi. Poiché 5 non divide 24 possiamo affermare che S_4 non ha sottogruppi di ordine 5. Infatti l'ordine di ogni suo sottogruppo deve appartenere all'insieme dei divisori di 24: $\{1, 2, 3, 4, 6, 12, 24\}$. Il teorema di Lagrange non afferma tuttavia che per ognuno di tali divisori esitono effettivamente sottogruppi con quell'ordine. Lasciamo come esercizio al lettore stabilire se in S_5 vi è un sottogruppo con 6 elementi.

§ 6.3 Omomorfismi strutture algebriche

Ora che consideriamo non solo insiemi, ma strutture algebriche (quindi un insieme dotato di un'operazione), ci interessa capire quando una funzione definita tra due strutture algebriche "rispetta" le operazioni.

Definizione 6.11. *Siano A, A' due insiemi e siano $*$ e $\star$ due operazioni definite su A e A' rispettivamente. Una funzione $f : A \to A'$ è un* **omomorfismo** *(detto anche* **morfismo***) rispetto alle operazioni $*$ e $\star$ se*

$$\forall a, b \in A, \quad f(a * b) = f(a) \star f(b).$$

Esempio 6.12. Si consideri la funzione $f : (\mathbb{Z}, +) \to (\mathbb{R}, \cdot)$ data da $f(a) = 2^a$. Possiamo verificare che f è un omomorfismo rispetto alle operazioni indicate. Infatti

$$\forall a, b \in \mathbb{Z}, \quad f(a + b) = 2^{a+b} = 2^a \cdot 2^b = f(a) \cdot f(b).$$

Esempio 6.13. Si consideri la funzione $\varphi : (\mathbb{Z}, \cdot) \to (\mathbb{R}, +)$ data da $\varphi(a) = a^2$. Possiamo verificare che φ non è un omomorfismo rispetto alle operazioni indicate mostrando che in almeno un caso non rispetta le operazioni. Ad esempio

$$\varphi(3 \cdot 5) = \varphi(15) = 15^2 = 225 \neq \varphi(3) + \varphi(5) = 3^2 + 5^2 = 34$$

Se una struttura algebrica deve soddisfare anche altre condizioni, oltre a possedere una operazione, una funzione sarà un omomorfismo di quella struttura se oltre alle operazioni rispetterà anche le altre proprietà.

Definizione 6.14. *Siano $(A, *)$ e $(B, \star)$ due semigruppi. Diremo che una funzione $f : A \to B$ è un* **omomorfismo di semigruppi** *se è un omomorfismo rispetto alle operazioni. Se inoltre $(A, *)$ e $(B, \star)$ sono monoidi e 1_A, 1_B indicano rispettivamente l'elemento neutro di A rispetto all'operazione $*$ e l'elemento neutro di B rispetto all'operazione $\star$, diremo che $f : A \to B$ è un* **omomorfismo di monoidi** *se è un omomorfismo di semigruppi e inoltre $f(1_A) = 1_B$.*

Esempio 6.15. Consideriamo $\mathbb{Z} \times \mathbb{Z}$ con l'operazione di moltiplicazione componente per componente $(a, b) \cdot (a', b') = (aa', bb')$. Siverifica facilmente che si tratta di un monoide con identit'a $(1, 1)$, ma non di un gruppo: ad esempio $(0, 0)$ è un elemento privo di inverso. Consideriamo la funzione $f \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ data da $f((a, b)) = (a, 0)$. Questa funzione rispetta l'operazione del monoide, ma non è un omomorfismo di monoidi, in quanto $f((1, 1)) = (1, 0)$ che non è l'identità del codominio.

§ 6.4 Omomorfismi di gruppi

Definizione 6.16. *Siano $(G, \cdot)$, $(K, \cdot)$ due gruppi. Una funzione $f \colon G \longrightarrow K$ si dice* **omomorfimo di gruppi** *se rispetta le operazioni, ossia:*

$$\forall a, b \in G : \quad f(a \cdot b) = f(a) \cdot f(b).$$

L'idea di omomorfismo di struttura algebrica è quella di una funzione che rispetta tutte le proprietà della struttura algebrica. Nel caso dei gruppi ci si aspetterebbe che la definizione contenga anche la richiesta di mandare l'identità del dominio in quella del codominio e di mandare l'inverso di un elemento nell'inverso della sua immagine. Vediamo ora che queste condizioni sono solo apparentemente assenti dalla definizione; in realtà nel caso dei gruppi la condizione di essere compatibile con le operazioni ha come conseguenza anche quelle relative alle identità e agli inversi.

Lemma 6.17. *Per ogni omomorfismo di gruppi $f \colon (G, \cdot) \longrightarrow (K, \cdot)$, si ha:*

i) $f(1_G) = 1_K$

ii) $f(a^{-1}) = f(a)^{-1}$

iii) $f(a^n) = f(a)^n$

Dimostrazione. Preso un qualsiasi elemento $a \in G$, avremo per definizione di omomorfismo e di identità:

$$f(a) \cdot f(1_G) = f(a \cdot 1_G) = f(a) = f(a) \cdot 1_K.$$

Applicando la cancellazione a $f(a) \cdot f(1_G) = f(a) \cdot 1_K$ otteniamo $f(1_G) = 1_K$. □

Si faccia attenzione al fatto che la dimostrazione del lemma precedente funziona perché dominio e codominio sono gruppi, ma non vale ad esempio nel caso dei monomidi, come si vede nell'esempio seguente. Non tutte le funzioni tra due gruppi sono omomorfismi. La funzione considerata nel lemma seguente in genere non lo è , tuttavia si tratta di una funzione importante, con conseguenze interessanti.

Definizione 6.18. *Un omomorfismo di gruppi si dice:*

- **epimorfismo** *se è suriettivo*
- **monomorfismo** *se è iniettivo*
- **isomorfismo** *se è biunivoco.*

Se esiste un isomorfismo tra i gruppi G e K, allora si dice che G e K sono isomorfi e si scrive $G \simeq K$.

Esempio 6.19. Il gruppo delle simmetrie del triangolo equilatero è isomorfo al gruppo S_3 delle permutazioni di 3 elementi. Si ottiene un isomorfismo numerando da 1 a 3 i vertici del triangolo ed associado ad ogni simmetria del triangolo la corrispondente permutazione dei vertici. Il gruppo delle simmetrie del quadrato non è invece isomorfo al gruppo S_4. Possiamo costruire un monomorfismo in modo analogo a quanto fatto per il triangolo equilatero. Tuttavia nessuna simmetria del quadrato corrisponde alla permutazione che fissa due vertici adiacenti e scambia gli altri due.

Abbiamo visto che una funzione è suriettiva se la sua immagine insiemistica coincide col codominio. Ovviamente questo vale anche per i morfismi di gruppi. Tuttavia l'insieme immagine in questo caso ha proprietà più interessanti.

Lemma 6.20. *Se* $f\colon (G, \cdot) \longrightarrow (K, \cdot)$ *è un omomorfismo di gruppi, allora l'immagine di* f *è un sottogruppo di* K*, In simboli:* $Im(f) < K$.

Dimostrazione. Eseguiamo la verifica utilizzando il Criterio dei sottogruppi. Due qualsiasi elementi di $Im(f)$ sono del tipo $f(a)$, $f(b)$ con $a, b \in G$. Abbiamo allora, grazie alla Proposizione 6.17 e alla definizione di omomorfismo:

$$f(a) \cdot f(b)^{-1} = f(a) \cdot f(b^{-1}) = f(a \cdot b^{-1}).$$

Poiché G è un gruppo e $a, b \in G$, allora anche $a \cdot b^{-1} \in G$ e quindi $f(a \cdot b^{-1}) \in Im(f)$. □

Per verificare l'iniettività di una funzione dobbiamo controllare che ogni coppia di elementi diversi del dominio abbiano immagini diverse. Nel caso dei morfismi il controllo puè essere fattopiù velocemente usando la nozione seguente.

Definizione 6.21. *Dato un omomorfismo di gruppi $f\colon (G, \cdot) \longrightarrow (K, \cdot)$, si dice* **nucleo** *di f e si denota $Ker(f)$ l'insieme controimmagine di 1_K. In simboli:*

$$Ker(f) := \{a \in G \mid f(a) = 1_K\}.$$

Lemma 6.22. *Sia $f\colon (G, \cdot) \longrightarrow (K, \cdot)$ un omomorfismo di gruppi. Allora:*

i) il nucleo di f è un sottogruppo di G. In simboli $Ker(f) < G$.

ii) f è un monomorfismo $\iff Ker(f) = \{1_G\}$.

Dimostrazione. i) Usiamo il criterio. Siano a, b due elementi di $Ker(f)$, ossia due elementi di G tali che $f(a) = f(b) = 1_K$. Allora:

$$f(a \cdot b^{-1}) = f(a) \cdot f(b^{-1}) = f(a) \cdot f(b)^{-1} = 1_K \cdot 1_K^{-1} = 1_K \cdot 1_K = 1_K.$$

Dunque $f(a \cdot b^{-1}) = 1_K$ ossia $a \cdot b^{-1} \in Ker(f)$. *ii)* "$\Longrightarrow$" Se f è iniettivo, la controimmagine di un elemento, in particolare la controimmagine di 1_K, contiene al massimo un elemento. D'altra parte $Ker(f)$ è un sottogruppo di G e quindi contiene almeno 1_G. Dunque $Ker(f) = \{1_G\}$. "$\Longleftarrow$" Supponiamo che f non sia iniettivo: esistono allora due elementi diversi a, b di G tali che $f(a) = f(b)$. Allora $f(a \cdot b^{-1}) = f(a) \cdot f(b)^{-1} = f(a) \cdot f(a)^{-1} = 1_K$. Dunque $a \cdot b^{-1} \in Ker(f)$ e $a\, b^{-1} \neq 1_G$. □

Corollario 6.23. *Nelle ipotesi del Lemma precedente, se $f(a) = c$, allora l'insieme controimmagine di c è*

$$f^{-1}(c) = \{a \cdot d \mid d \in Ker(f)\} = \{d \cdot a \mid d \in Ker(f)\}.$$

Dimostrazione. Proviamo solo la prima uguaglianza; la seconda è del tutto analoga. Per "$\supseteq$"basta osservare che $f(a \cdot d) = f(a) \cdot f(d) = c \cdot 1_K = c$. "$\subseteq$"Sia $a' \in G$ tale che $f(a') = c$. Allora $f(a^{-1} \cdot a') = f(a)^{-1} \cdot f(a') = c^{-1} \cdot c = 1_K$. Dunque $a^{-1} \cdot a' \in Ker(f)$. Ponendo $d := a^{-1} \cdot a' \in Ker(f)$, otteniamo $a' = (a \cdot a^{-1}) \cdot a' = a \cdot (a^{-1} \cdot a') = a \cdot d$. □

§ 6.5 Gruppi ciclici

Lemma 6.24. *Sia $(G, \cdot)$ un gruppo ed a un suo elemento. Il sottoinsieme $H := \{a^n \mid n \in \mathbb{Z}\}$ di G è un suo sottogruppo.*

Dimostrazione. Usiamo il criterio dei sottogruppi. Se a^n e a^m sono due qualsiasi elementi di H, allora il prodotto del primo per l'inverso del secondo è $a^n \cdot (a^m)^{-1} = a^n \cdot a^{-m} = a^{n-m}$ (Corollario 4.30) e quindi appartiene ad H . □

Definizione 6.25. *Sia $(G, \cdot)$ un gruppo e a un suo elemento. Si dice* **sottogruppo ciclico generato da** *a e si denota con $\langle a \rangle$ il sottogruppo costituito dalle potenze di a con esponenti interi. Diremo che G è un* **gruppo ciclico** *se vi è un suo elemento a tale che $G = \langle a \rangle$.*

Attenzione: In notazione additiva, ossia se il gruppo è $(G, +)$, scriveremo

$$G =< g >= \{ng \mid n \in \mathbb{Z}\}.$$

Esempio 6.26. Il sottoinsieme $5\mathbb{Z}$ dei multipli interi di 5 è un sottogruppo ciclico di $(\mathbb{Z}, +)$. Infatti in notazione additiva elevare a potenza n-esima un elemento significa sommarlo con se stesso n volte se $n > 0$ e significa sommare con se stesso $(-n)$-volte il suo opposto se $n < 0$; infine se $n = 0$ la potenza con esponente 0 è per definizione l'identità del gruppo, ossia nel nostro caso è 0. Quindi in notazione additiva la potenza n-esima di x si scrive nx e in questo caso è proprio il prodotto di n per x. Dunque i multipli di 5 costituiscono il sottogruppo ciclico generato da 5 nel gruppo $\mathbb{Z}$ con l'operazione di addizione. Notiamo che $(\mathbb{Z}, +)$ stesso è un gruppo ciclico perché coincide col suo sottogruppo ciclico generato da 1.

Esempio 6.27. Nel gruppo delle permutazioni S_5 il sottogruppo ciclico generato dal ciclo $\sigma = (1 \;\; 4 \;\; 2)$ contiene 3 elementi, ed esattamente $\langle \sigma \rangle = \{1_{S_5} = \sigma^0, \sigma = \sigma^1, (1 \;\; 2 \;\; 4) = \sigma^2\}$. Infatti si può verificare che $\sigma^3 = 1_{S_5}$ e quindi tutte le potenze con esponenti interi positivi coincidono con uno dei 3 elementi scritti. Inoltre da $\sigma^3 = 1_{S_5}$ si deduce anche che $\sigma^2 = \sigma^{-1}$ e quindi anche le potenze di σ con esponenti negativi coincidono con una delle 3 potenze elencate.

Proposizione 6.28. *Sia σ un r-ciclo del gruppo simmetrico S_n. Il sottogruppo ciclico generato da σ ha esattamente r elementi:*

$$\langle \sigma \rangle = \{1_{S_n} = \sigma^0, \sigma = \sigma^1, \sigma^2, \ldots, \sigma^{r-1}\}.$$

Dimostrazione. Sia $\sigma = (c_1 \;\; c_2 \;\; \ldots \;\; c_r)$. Possiamo intanto osservare che $\sigma^r = 1_{S_n}$ e quindi, generalizzando il ragionamento fatto nell'esempio precedente, ogni potenza di σ coincide con una di quelle elencate. Inoltre tutte le potenze elencate sono diverse; infatti se $0 \leq n < m \leq r - 1$ abbiamo $\sigma^n(c_1) = c_n \neq \sigma^m(c_1) = c_m$. Quindi $\sigma^n \neq \sigma^m$. □

Esempio 6.29. Il gruppo $(\mathbb{Z}, +)$ contiene oltre ai sogruppi banali, ossia al sottogruppo nullo che contiene solo 0 e il sottogruppo che coincide con tutto $\mathbb{Z}$, anche tanti altri sottogruppi ciclici. Per ogni $n \geq 0$, il sottoinsieme di $\mathbb{Z}$ dei multipli interi di n:

$$n\mathbb{Z} := \{nt \mid t \in \mathbb{Z}\}$$

è un sottogruppo di $(\mathbb{Z}, +)$. Nei prossimi capitoli vedremo che questi sono tutti i possibili sottogruppi di $(\mathbb{Z}, +)$. Cosideriamo per ora un caso particolare. Il sottoinsieme $H := \{6h+9k \mid h, k \in \mathbb{Z}\} \subset \mathbb{Z}$ à un sottogruppo di $(\mathbb{Z}, +)$. Presi infatti due qualsiasi elementi $6h+9k$ e $6h'+9k'$ di H, avremo $(6h+9k)-(6h'+9k') = 6(h-h')+9(k-k') \in H$. Mostriamo ora che H coincide col sottogruppo ciclico $3\mathbb{Z}$. L'inclusione $H \subseteq 3\mathbb{Z}$ à evidente: tutti gli elementi di H sono multipli di 3: $6h + 9k = 3(2h + 3k)$. L'altra inclusione si ottiene osservando che $3 = 6 \cdot 2 + 9 \cdot (-1) \in H$ e quindi per ogni $t \in \mathbb{Z}$ si ha $3t = 6 \cdot 2t + 9 \cdot (-t) \in H$.

§ 6.6 Periodo di un elemento

Consideriamo ora un elemento g di un gruppo $(G, \cdot)$ e le sue potenze. Se vi sono due esponenti diversi $n \neq m$ tali che $g^n = g^m$, allora per la potenza con esponente la loro differenza si ha $g^{n-m} = g^n \cdot (g^m)^{-1} = g^n \cdot (g^n)^{-1} = 1_G$. In particolare supponendo $n > m$, avremo una potenza di g con esponente positivo che vale 1_G.

Definizione 6.30. *Diremo che g ha* **periodo infinito** *se tutte le potenze di g sono tutte diverse. In caso contrario si dice* **periodo di** *g il minimo intero positivo v tale che $g^v = 1_G$.*

In notazione additiva, ossia se $g \in (G, +)$, il periodo di g à il minimo intero positivo v tale che $vg = 0_G$ (oppure à infinito).

Esempio 6.31. Consideriamo il gruppo S_5 delle permutazioni di $\{1, 2, 3, 4, 5\}$ con l'usuale composizione. Componendo con sé stessa la permutazione $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix}$ otteniamo $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \end{pmatrix}$ e $\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = Id$. Dunque il peiodo di σ à 3.

Lemma 6.32. *L'identità 1_G di un gruppo $(G, \cdot)$ à l'unico elemento con periodo 1. Il periodo di un elemento $g \in G$, $g \neq 1_G$, coincide con l'ordine del sottogruppo ciclico generato da g, ossia:*

- *g ha ordine infinito $\iff < g > \simeq \mathbb{Z}$*
- *g ha ordine finito k allora $< g >$ ha k elementi.*

Dimostrazione. Consideriamo l'omomorfismo $\varphi\colon \mathbb{Z} \longrightarrow G$ definito da associando ad ogni $k \in \mathbb{Z}$ la potenza g^k. Se g ha ordine finito k allora $< g >$ è costituito dalle potenze di g con esponenti da 0 a $k-1$. □

Corollario 6.33. *Il periodo di un qualsiasi elemento di un gruppo finito G di ordine n è un divisore di n.*

§ 6.7 Alcuni gruppi importanti

I gruppi diedrali

Si dicono **gruppi diedrali** i gruppi di simmetrie di un dato poligono i Possiamo considerare ad esempio le simmetrie del triangolo isoscele, oppure quelle dell'esagono regolare o quelle di un rettangolo non quadrato e cosı via. Un modo semplice per individuare le simmetrie di un poligono è quello di etichettare i suoi vertici (ad esempio ordinatamente con i numeri da 1 a n) e di considerare quindi la permutazione dei vertici corrispondente a ciascuna simmetria. 'E facile verificare che in questo modo le simmetrie di un triangolo rettangolo corrispondono all'intero gruppo S_3. Invece per $n \geq 4$, e simmetrie di un poligono regolare con n lati corrispondono ad un sottogruppo proprio di S_n di cardinalità $2n$: ci sono n vertici in cui "spostare" il vertice etichettato con 1 e per ciascuno ci sono due vertici, quelli a lui adiacenti, in cui spostare il vertice 2.

Le classi di resto $\mathbb{Z}_n$

Sia n un intero fissato, $n \geq 2$. Indichiamo con $n\mathbb{Z}$ l'insieme dei multipli interi di n, ossia $n\mathbb{Z} = \{nt \mid t \in \mathbb{Z}\}$. Possiamo associare a n (o a $n\mathbb{Z}$) la relazione di **congruenza modulo** n in $\mathbb{Z}$:

$$a\, R_n\, b \quad \text{se e solo se} \quad a - b \in n\mathbb{Z}.$$

Se $a\, R_n\, b$ si dice che a **è congruo a** b **modulo** n e si scrive $a \equiv b \bmod n$. Un modo equivalente di esprimere la relazione di congruenza modulo n è la seguente:

$a \equiv b \bmod n$ se e solo se le divisioni di a e di b per n hanno lo stesso resto r.

Infatti, se $a = nq + r$ e $b = nq' + r$, allora $a - b = n(q - q') \in n\mathbb{Z}$; viceversa se $b = a + nt$ e $a = nq + r$, anche la divisione di b per n, ossia $b = n(q + t) + r$, ha lo stesso resto r. Tratteremo più a fondo la divisione con resto in uno dei prossimi capitoli. La relazione di congruenza modulo n è una relazione di equivalenza in $\mathbb{Z}$. Il quoziente si dice **insieme delle classi di resto modulo** n (o delle classi di congruenza modulo n) e si indica abitualmente con $\mathbb{Z}_n$.

Lemma 6.34. i) *Se $[a] \in \mathbb{Z}_n$, allora $[a] = \{a + nt \mid t \in \mathbb{Z}\}$.*

ii) *$\mathbb{Z}_n$ ha esattamente n classi distinte. Più precisamente* $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$.

Dimostrazione. La prima parte dell'asserto segue immediatamente dalla definizione di congruenza data inizialmente: $b \equiv a \bmod n$ se e solo se $b - a \in n\mathbb{Z}$ ossia se e solo se $b = a + nt$ con $t \in \mathbb{Z}$. La seconda parte dell'asserto si ottiene ricordando che ogni classe di equivalenza $[a]$ è caratterizzata dal resto della divisione di a per n e che i resti possibili sono gli interi r tali che $0 \leq r < n$. □

Possiamo definire in $\mathbb{Z}_n$ delle operazioni di somma e prodotto ponendo:

$$[a] + [b] = [a + b] \text{e analogamente} [a] \cdot [b] = [ab].$$

Lasciamo come esercizio al lettore la verifica che queste operazioni sono ben definite, ossia che il risultato non dipende dai rappresentanti. Le classi di resto $\mathbb{Z}_n$ con l'operazione di somma prima definita è un gruppo abeliano. L'identità è $[0]$ e l'opposto di una classe $[a]_n$ é la classe che ha come rappresentante l'opposto, ossia $-[a]_n = [-a]_n$.

Esempio 6.35. Scriviamo esplicitamente le tabelline della somma nei casi $n = 3$ e $n = 2$. Per semplicità nelle tabelline scriviamo solo i numeri che sono rappresentanti speciali delle classi, sottointendendo il simbolo che indica la classe.

Tabellina di$\mathbb{Z}_3$:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Tabellina di$\mathbb{Z}_4$:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Otteniamo due tabelline simmetriche rispetto alla diagonale principale poiché l'operazione è commutativa. Osserviamo anche che in ogni riga ed in ogni colonna compaiono tutti gli elementi, ma scritti ogni volta in un diverso ordine.

Il risultato delle operazioni + e $\cdot$ in $\mathbb{Z}_n$ non sempre è "intuitivo".

Esempio 6.36. Scriviamo la tabella delle operazioni + e $\cdot$ in $\mathbb{Z}_6$:

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[2]$	$[0]$	$[2]$	$[4]$	$[0]$	$[2]$	$[4]$
$[3]$	$[0]$	$[3]$	$[0]$	$[3]$	$[0]$	$[3]$
$[4]$	$[0]$	$[4]$	$[2]$	$[0]$	$[4]$	$[2]$
$[5]$	$[0]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

Possiamo anche considerare $\mathbb{Z}_n$ con l'operazione di prodotto sui rappresentanti: $[a]_n \cdot [b]_n := [ab]_n$. Però $(\mathbb{Z}_n, \cdot)$ non è un gruppo. Infatti $[1]_n$ è l'identità rispetto al prodotto, ma $[0]_n$ non ha l'inverso.

§ 6.8 Esercizi

6.1 Consideriamo la funzione $f : \mathbb{R} \to \mathbb{R}$ definita come $f(x) := 2x$.
Consideriamo $\mathbb{R}$ con l'operazione $+$. La funzione f è un omomorfismo di $(\mathbb{R}, +)$ in sé stesso? 'E anche un omomorfismo di monoidi?
Consideriamo $\mathbb{R}$ con l'operazione $\cdot$. La funzione f è un omomorfismo di $(\mathbb{R}, \cdot)$ in sé stesso? 'E anche un omomorfismo di monoidi?

6.2 Consideriamo l'insieme $\{1, -1\}$ e l'usuale operazione prodotto $\cdot$. $(\{1, -1\}, \cdot)$ è un semigruppo? 'E anche un monoide?

6.3 Consideriamo i monoidi $(\mathbb{Z}, +)$ e $(\{1, -1\}, \cdot)$ e la funzione $f : \mathbb{Z} \to \{1, -1\}$,

$$f(a) = \begin{cases} 1 & \text{se } a \text{ è pari} \\ -1 & \text{se } a \text{ è dispari} \end{cases}$$

f è un omomorfismo di monoidi?

6.4 Consideriamo la funzione $f : \mathbb{R}^+ \setminus \{0\} \to \mathbb{R}$ definita come $f(x) := \log(x)$. Consideriamo $\mathbb{R}^+ \setminus \{0\}$ con l'operazione $+$ e $\mathbb{R}$ con l'operazione $\cdot$. La funzione f è un omomorfismo?

6.5 Sia A un insieme e sia $(W_A, \circ)$ il monoide libero delle parole su A. Definiamo la funzione **lunghezza di una parola**:

$$\begin{array}{rcl} \lambda : W_A & \to & \mathbb{N} \\ w = a_1 \dots a_n & \mapsto & n. \end{array}$$

Se consideriamo $\mathbb{N}$ con l'operazione $+$, λ è un omomorfismo di monoidi?

6.6 Si consideri la struttura algebrica $(\mathbb{Z}, \circ)$, dove l'operazione $\circ$ è definita come segue:

$$\forall x, y \in \mathbb{Z}, \quad x \circ y = xy + x.$$

1. Stabilire se $\circ$ è un'operazione associativa e/o commutativa;
2. determinare l'eventuale elemento neutro della struttura algebrica $(\mathbb{Z}, \circ)$;

3. se la struttura algebrica $(\mathbb{Z}, \circ)$ ammette elemento neutro, determinare gli (eventuali) elementi di $\mathbb{Z}$ che hanno inverso rispetto alla legge $\circ$;
4. concludere se la struttura algebrica $(Z, \circ)$ è un monoide o un gruppo (abeliano?).

6.7 Sia S_4 il gruppo delle permutazioni di $\{1, 2, 3, 4\}$ con l'usuale composizione. Scrivere tutti gli elementi del gruppo ciclico H generato da $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$.

6.8 Nel gruppo S_5 delle permutazioni di $\{1, 2, 3, 4, 5\}$ con l'usuale composizione, determinare il peiodo di $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$ e di $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}$.

6.9 Sia $(G, \cdot)$ un gruppo abeliano e siano $a, b \in G$.

(a) Provare che se a e b hanno periodo finito anche ab ha periodo finito.

(b) Provare che l'insieme H degli elementi di G con periodo finito formano un sottogruppo.

6.10 Sia $(G, \cdot)$ un gruppo e siano $a, b, c \in G$.

(a) Provare che a e a^{-1} hanno lo stesso periodo.

(b) Provare che ab e ba hanno lo stesso periodo.

6.11 Si consideri in $\mathbb{Q}$ l'operazione $\triangle$ definita da $a \triangle b = ab + a + b$.

(a) perché $(\mathbb{Q}, \triangle)$ non è un gruppo?

(b) Verificare che $(\mathbb{Q}^*, \triangle)$ è un gruppo.

6.12 Si consideri in $\mathbb{Z}$ l'operazione $\bullet$ definita da $a \bullet b = a + b - 1$. È vero che $(\mathbb{Z}, \bullet)$ è un gruppo?

6.13 Si consideri in $\mathbb{Z}$ l'operazione $*$ definita da $a * b = ab + a + b$.

(a) Verificare che $*$ è associativa e commutativa e ammette elemento neutro.

(b) È vero che $(\mathbb{Z}, *)$ è un gruppo?

6.14 Sia $M = \{\frac{1+4m}{1+4n} \ / \ n, m \in \mathbb{Z}\}$ dotato dell'usuale operazione di prodotto. Verificare che M è un gruppo.

6.15 Sia $H = \{a + \sqrt{2}b \mid a, b \in \mathbb{Q}\}$. Dimostrare che H è un sottogruppo di $(\mathbb{R}, +)$. È vero che $H - \{0\}$ è un sottogruppo del gruppo moltiplicativo $\mathbb{R}^*$?

6.16 Il gruppo prodotto Siano $(G, \cdot)$ e $(H, \cdot)$ due gruppi. Provare che l'operazione nell'insieme prodotto cartesiano $G \times K$ definita da $(a, b) \cdot (a', b') := (a \cdot a', b \cdot b')$ rende $G \times K$ un gruppo. Se non diversamente specificato, il prodotto cartesiano di due gruppi viene sempre considerato dotato di questa struttura di gruppo e viene chiamato *gruppo prodotto*. Verificare che le funzioni di proiezione π_1, π_2 dal prodotto cartesiano su uno dei fattori, nel caso di un gruppo prodotto sono degli epimorfismo di gruppi.

6.17 Consideriamo i gruppi additivi $\mathbb{Z}$, $\mathbb{Z}_6$ e $\mathbb{Z}_5$ e sia $f\colon (\mathbb{Z}, +) \to (\mathbb{Z}_6 \times \mathbb{Z}_5, +)$ definita da $f(n) = ([2n]_6 \ , \ [3n]_5)$.

(a) Verificare che si tratta di un omomorfismo di gruppi.

(b) Determinarne nucleo e immagine.

(c) Determinare il numero di elementi e un rappresentante per ogni classe di $\mathbb{Z}/Ker(f)$.

6.18 Si consideri in $G = S_3 \times \mathbb{Z}_6$ l'operazione definita da $(\sigma, \overline{a}) * (\tau, \overline{b}) = (\sigma\tau, \overline{a+b})$.

(a) Verificare che G è un gruppo. E' abeliano?

(b) Dire se $H = S_3 \times \{\overline{0}\}$, $K = S_3 \times \{\overline{1}\}$, $M = \{1_{S_3}\} \times \mathbb{Z}_6$ sono sottogruppi ed in caso affermativo se sono abeliani.

6.19 Consideriiamo i gruppi additivi $\mathbb{Z}_9$ e $\mathbb{Z}_{12}$. Indichiamo con $[n]$ la classe di un numero intero n in $\mathbb{Z}_9$ e con $\overline{n}$ la sua classe in $\mathbb{Z}_{12}$.

(a) Provare che $f : \mathbb{Z}_9 \to \mathbb{Z}_{12}$ tale che $f([n]) = \overline{n^2}$ non è una funzione ben definita. Verificare che invece lo è $g : \mathbb{Z}_9 \to \mathbb{Z}_{12}$ data da $g([n]) = \overline{4n}$.

(b) Determinare $Im(g)$, $g^{-1}(\overline{0})$ e $g^{-1}(\overline{1})$. g è un omomorfismo di gruppi?

(c) Determinare tutti i possibili omomorfismi di gruppi da $\mathbb{Z}_9$ in $\mathbb{Z}_{12}$.

6.20 Consideriiamo i gruppi additivi $\mathbb{Z}_8$ e $\mathbb{Z}_{12}$. Indichiamo con $[n]$ la classe di un numero intero n in $\mathbb{Z}_8$ e con $\overline{n}$ la sua classe in $\mathbb{Z}_{12}$.

(a) Provare che $f : \mathbb{Z}_{12} \to \mathbb{Z}_8$ tale che $f(\overline{n}) = [4n^2]$ è una funzione ben definita e che è un omomorfismo di gruppi.

(b) Determinare $Im(f)$, $Ker(f)$ e gli insiemi controimmagine di ogni elemento del codominio.

6.21 Sia S_3 il gruppo delle permutazioni di 3 elementi e sia $g\colon S_3 \to S_3$ definito da $\sigma \mapsto \sigma^2$.

(a) Determinare $g^{-1}(1_{S_3})$.

(b) Verificare che g non è un omomorfismo di gruppi.