Lezione 17

Prerequisiti: Lezioni 2-4, 8.

Elementi periodici.
Teoremi di Lagrange, Eulero e Fermat.
Gruppi ciclici.

Definizione 17.1 Sia $(G,+)$ un gruppo additivo. Sia $g \in G$. Per ogni $n \in \mathbb{Z}$ si pone

$$ng = \begin{cases} 0_G & \text{se } n = 0; \\ \underbrace{g + \cdots + g}_{n \text{ volte}} & \text{se } n > 0; \\ -\big((-n)g\big) & \text{se } n < 0. \end{cases}$$

Tale elemento si dice *n-esimo multiplo di g*. Il numero *n* si dice *fattore* del multiplo.

Osservazione 17.2 Quando $n > 0$, la definizione di *ng* si può dare mediante una formula ricorsiva, ponendo

$$1g = g \text{ e, per ogni } n > 1,\ ng = (n-1)g + g. \tag{1}$$

Tale formula è utile alla dimostrazione del seguente enunciato, la cui verifica è lasciata per esercizio al lettore.

Proposizione 17.3* *(Proprietà dei multipli)* Sia $(G,+)$ un gruppo additivo. Allora

(a) per ogni $g \in G$, ed ogni $n \in \mathbb{Z}$, $(-n)g = -(ng)$;

(b) per ogni $n \in \mathbb{Z}$, $n0_G = 0_G$;

(c) per ogni $g \in G$, ed ogni $n, m \in \mathbb{Z}$,

  (i) $(n+m)g = ng + mg$;

  (ii) $n(mg) = (nm)g$;

(d) per ogni $g, h \in G$ tali che $g + h = h + g$, e per ogni $n \in \mathbb{Z}$, si ha $n(g+h) = ng + nh$.

Diamo ora le versioni moltiplicative della Definizione 17.1, dell'Osservazione 17.2 e della Proposizione 17.3. Ricordiamo che la trascrizione dal caso additivo al caso moltiplicativo avviene sostituendo la somma di elementi del gruppo con il prodotto, lo zero del gruppo con l'uno del gruppo, l'opposto con l'inverso.

Definizione 17.4 Sia $(G,\cdot)$ un gruppo moltiplicativo. Sia $g \in G$. Per ogni $n \in \mathbb{Z}$ si pone

$$g^n = \begin{cases} 1_G & \text{se } n = 0; \\ \underbrace{g \cdots g}_{n \text{ volte}} & \text{se } n > 0; \\ \left(g^{-n}\right)^{-1} & \text{se } n < 0. \end{cases}$$

Tale elemento si dice *n-esima potenza di g*. Il numero *n* si dice *esponente* della potenza.

Osservazione 17.5 Quando $n > 0$, la definizione di g^n si può dare mediante una formula ricorsiva, ponendo

$$g^1 = g \text{ e, per ogni } n > 1, \quad g^n = g^{n-1} g. \tag{2}$$

Proposizione 17.6* *(Proprietà delle potenze)* Sia $(G,\cdot)$ un gruppo moltiplicativo. Allora

(a) per ogni $g \in G$, ed ogni $n \in \mathbb{Z}$, $g^{-n} = (g^n)^{-1}$;

(b) per ogni $n \in \mathbb{Z}$, ${1_G}^n = 1_G$;

(c) per ogni $g \in G$, ed ogni $n, m \in \mathbb{Z}$,

(i) $g^{n+m} = g^n g^m$;

(ii) $(g^n)^m = g^{nm}$;

(d) per ogni $g, h \in G$ tali che $gh = hg$, e per ogni $n \in \mathbb{Z}$, si ha $(gh)^n = g^n h^n$.

Esempio 17.7 Sia $n \in \mathbb{Z}$.

(a) Nel gruppo $(\mathbb{Z},+)$, l'*n*-esimo multiplo di 1 è $n \cdot 1 = n$.

(b) Nel gruppo $(\mathbb{Z}_2,+)$, l'*n*-esimo multiplo di $[1]_2$ è $n[1]_2 = [n]_2 = \begin{cases} [0]_2 & \text{se } n \text{ è pari;} \\ [1]_2 & \text{se } n \text{ è dispari.} \end{cases}$

Riassumendo: nel gruppo $(\mathbb{Z},+)$, l'unico multiplo di 1 ad essere uguale a zero è quello con fattore nullo, nel gruppo $(\mathbb{Z}_2,+)$ l'elemento $[1]_2$ ha, invece, infiniti multipli uguali a zero. A questi due casi si riferisce la nozione introdotta dalle seguenti definizioni, che ne danno le versioni additiva e moltiplicativa.

Definizione 17.8 Sia $(G,+)$ un gruppo additivo. Sia $g \in G$. Allora *g* si dice *aperiodico* se, per ogni $n \in \mathbb{Z}$,

$$ng = 0_G \Rightarrow n = 0.$$

Altrimenti *g* si dice *periodico*.

Definizione 17.9 Sia $(G,\cdot)$ un gruppo moltiplicativo. Sia $g \in G$. Allora *g* si dice *aperiodico* se, per ogni $n \in \mathbb{Z}$,

$$g^n = 1_G \Rightarrow n = 0.$$

Altrimenti *g* si dice *periodico*.

Dall'Esempio 17.7 sappiamo che, in base alla Definizione 17.8, l'elemento 1 del gruppo $(\mathbb{Z},+)$ è aperiodico, l'elemento $[1]_2$ nel gruppo $(\mathbb{Z}_2,+)$ è, invece, periodico. Forniamo ora esempi nel caso moltiplicativo. Tra i gruppi moltiplicativi includiamo anche, per ogni intero $n \geq 1$, il gruppo simmetrico $(S_n,\circ)$. Considereremo, d'ora in poi, anche nella scrittura, la composizione $\circ$ come un prodotto.

Esempio 17.10 Sia $n \in \mathbb{Z}$.
(a) Nel gruppo $(\mathbb{Q}^*,\cdot)$, l'*n*-esima potenza di 2 è 2^n.
(b) Nel gruppo $(S_2,\cdot)$, l'*n*-esima potenza di $\alpha = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ è $\alpha^n = \begin{cases} id & \text{se } n \text{ è pari;} \\ \alpha & \text{se } n \text{ è dispari.} \end{cases}$

Quindi, alla luce della Definizione 17.9, l'elemento 2 del gruppo $(\mathbb{Q}^*,\cdot)$ è aperiodico, l'elemento α nel gruppo $(S_2,\cdot)$ è, invece, periodico.

Esercizio 17.11 Dimostrare che, nel gruppo $(S_3,\cdot)$, l'elemento $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ è periodico.

Svolgimento: Calcoliamo le potenze di σ. Si ha

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

$$\sigma^3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^2\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = id.$$

Dunque la terza potenza di σ è l'elemento uno di S_3. Ciò prova che σ è periodico.

In base alle Definizioni 17.8 e 17.9, ogni elemento periodico ha, nel caso additivo, un multiplo con fattore *non nullo* uguale all'elemento zero, e, nel caso moltiplicativo, una potenza con esponente *non nullo* uguale all'elemento uno.

Negli Esempi 17.7 (b), 17.10 (b) e l'Esercizio 17.11 gli elementi periodici considerati hanno, però, nel caso additivo, un multiplo con fattore *positivo* uguale all'elemento zero, e, nel caso moltiplicativo, una potenza con esponente *positivo* uguale all'elemento uno. Ciò corrisponde ad una proprietà generale degli elementi periodici. La presentiamo includendo, in un unico enunciato, sia la versione additiva, sia quella moltiplicativa.

Lemma 17.12 Sia $(G,+)$ un gruppo additivo. Sia *g* un elemento periodico. Allora esiste un intero positivo n tale che $ng = 0_G$.
(Sia $(G,\cdot)$ un gruppo moltiplicativo. Sia *g* un elemento periodico. Allora esiste un intero positivo n tale che $g^n = 1_G$.)

Dimostrazione: (Caso additivo). Essendo *g* un elemento periodico, esiste un intero non nullo *n* tale che $ng = 0_G$. Se $n > 0$, la tesi è provata. Se $n < 0$, allora, in base alla Definizione 17.1, $(-n)g = -(ng) = -0_G = 0_G$. Essendo $-n > 0$, la tesi è provata anche in questo caso. □

La "periodicità" di un elemento periodico può essere misurata con un opportuno numero.

Definizione 17.13 Sia $(G,+)$ un gruppo additivo. Sia g un elemento periodico. Si dice *periodo* di g il numero

$$o(g) = \min\left\{n \in \mathbb{Z}, n > 0 \middle| ng = 0_G\right\}.$$

(Sia $(G,\cdot)$ un gruppo moltiplicativo. Sia g un elemento periodico. Si dice *periodo* di g il numero

$$o(g) = \min\left\{n \in \mathbb{Z}, n > 0 \middle| g^n = 1_G\right\}.)$$

Osservazione 17.14 La precedente definizione è ben posta, in quanto, in base al Lemma 17.12, gli insiemi citati nella Definizione 17.13 sono sottoinsiemi non vuoti di $\mathbb{N}$, e quindi ad essi si applica il principio del minimo.

Esempio 17.15 (a) In un qualsiasi gruppo additivo o moltiplicativo, l'unico elemento periodico di periodo 1 è l'elemento neutro.
(b) In base all'Esempio 17.7 (b), il periodo dell'elemento $[1]_2$ di $(\mathbb{Z}_2,+)$ è pari a 2; in base all'Esempio 17.10 (b), il periodo dell'elemento $\alpha = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ di $(S_2,\cdot)$ è pari a 2; in base all'Esercizio 17.11, il periodo dell'elemento $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ di $(S_3,\cdot)$ è pari a 3.

Nell'Esempio 17.7 (b) abbiamo visto che i multipli di $[1]_2$ che sono uguali a zero sono tutti e soli quelli il cui fattore è multiplo di 2, cioè, del periodo dell'elemento. Ciò corrisponde ad una proprietà generale.

Proposizione 17.16 *(Caratterizzazione del periodo)* Sia $(G,+)$ un gruppo additivo. Sia g un elemento periodico. Allora, per ogni $n \in \mathbb{Z}$,

$$ng = 0_G \text{ se e solo se } o(g) \text{ divide } n.$$

(Sia $(G,\cdot)$ un gruppo moltiplicativo. Sia g un elemento periodico. Allora, per ogni $n \in \mathbb{Z}$,

$$g^n = 1_G \text{ se e solo se } o(g) \text{ divide } n.)$$

Dimostrazione: (Caso additivo) Sia $n \in \mathbb{Z}$, e siano q ed r, rispettivamente, il quoziente ed il resto della divisione euclidea di n per $o(g)$. Allora

$$ng = (o(g)q + r)g = (o(g)q)g + rg = (qo(g))g + rg = q(o(g)g) + rg = rg,$$

dove abbiamo utilizzato, nell'ordine, la Proposizione 17.3 (c) (i) e (ii), la Definizione 17.13 e la Proposizione 17.3 (b). Ora, se $rg = 0$, allora, essendo $r < o(g)$, r non può essere positivo, e dunque $r = 0$. In tal caso $o(g)$ divide n. Viceversa, se $o(g)$ divide n, allora $r = 0$, e quindi, in base alla Definizione 17.1, $rg = 0$. □

Corollario 17.17 *(Periodicità)* Sia $(G,+)$ un gruppo additivo. Sia g un elemento periodico. Allora, per ogni $m,n\in\mathbb{Z}$,

$$ng = mg \quad \text{se e solo se} \quad n \equiv m \pmod{o(g)}.$$

(Sia $(G,\cdot)$ un gruppo moltiplicativo. Sia g un elemento periodico. Allora, per ogni $n,m\in\mathbb{Z}$,

$$g^n = g^m \quad \text{se e solo se se} \quad n \equiv m \pmod{o(g)}.)$$

Dimostrazione: (Caso additivo) Siano $m,n\in\mathbb{Z}$. Allora, in base alla Proposizione 17.3 (a) e (c) (i) ed alla Proposizione 17.16,

$$ng = mg \Leftrightarrow ng - mg = 0_G \Leftrightarrow (n-m)g = 0_G \Leftrightarrow o(g) \text{ divide } n-m \Leftrightarrow n \equiv m \pmod{o(g)}. \square$$

Corollario 17.18 *(Aperiodicità)* Sia $(G,+)$ un gruppo additivo. Sia g un elemento aperiodico. Allora, per ogni $m,n\in\mathbb{Z}$,

$$ng = mg \quad \text{se e solo se} \quad n = m.$$

(Sia $(G,\cdot)$ un gruppo moltiplicativo. Sia g un elemento aperiodico. Allora, per ogni $n,m\in\mathbb{Z}$,

$$g^n = g^m \quad \text{se e solo se} \quad n = m.\ )$$

Dimostrazione: (Caso additivo) Siano $m,n\in\mathbb{Z}$. Allora, in base alla Proposizione 17.3 (a), (b) e (c) (i) ed alla Definizione 17.8,

$$ng = mg \Leftrightarrow ng - mg = 0_G \Leftrightarrow (n-m)g = 0_G \Leftrightarrow n-m = 0 \Leftrightarrow n = m. \square$$

Il Corollario 17.17 chiarisce l'origine del termine *periodico*: i multipli (o le potenze) di un elemento periodico si ripetono, ciclicamente, secondo la classe di congruenza modulo il *periodo* del fattore (o dell'esponente). Tale ripetizione è invece assente nel caso di un elemento aperiodico, i cui multipli (le cui potenze) sono a due a due distinti.

Diamo ora alcune applicazioni del periodo alla teoria dei gruppi e all'aritmetica dei numeri interi.

Teorema 17.19 *(Teorema di Lagrange per i gruppi abeliani finiti)* Sia G un gruppo abeliano finito, e sia $g\in G$. Allora g è periodico, e $o(g)$ divide $|G|$.

Dimostrazione: Utilizzeremo la notazione moltiplicativa. Sia $s=|G|$, e sia $G=\{a_1,...,a_s\}$. Definiamo l'applicazione $\varphi: G\to G$ ponendo, per ogni $a\in G$, $\varphi(a)=ga$. Allora φ è bigettiva, avendo come inversa l'applicazione $\psi: G\to G$ tale che, per ogni $a\in G$, $\psi(a)=g^{-1}a$. Si ha dunque che $G=\operatorname{Im}\varphi=\{\varphi(a_1),...,\varphi(a_s)\}=\{ga_1,...,ga_s\}$. Pertanto

$$a_1a_2\cdots a_s = (ga_1)(ga_2)\cdots(ga_s).$$

Applicando, a secondo membro, le proprietà associativa e commutativa, si ottiene l'uguaglianza

$$a_1 a_2 \cdots a_s = g^s (a_1 a_2 \cdots a_s).$$

Cancellando, su entrambi i membri, l'elemento $a_1 a_2 \cdots a_s$, si ottiene $1_G = g^s$, e quindi, essendo $s > 0$, g è periodico e, in base alla Proposizione 17.16, $o(g)$ divide $s = |G|$. □

Nota Ricordiamo che, se G è un gruppo finito, il numero $|G|$ si dice *ordine* di G. L'ultima parte dell'enunciato del Teorema 17.19 si può dunque riassumere dicendo che, *in un gruppo finito, il periodo di ogni elemento divide l'ordine del gruppo.*

Esempio 17.20 Nell'Esercizio 17.11 abbiamo visto che, nel gruppo $(S_3, \cdot)$, l'elemento $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ è periodico di periodo 3. In effetti, questo è un divisore dell'ordine di S_3 che, in base alla Proposizione 4.6, è pari a 6. Si può dimostrare che il Teorema 17.19 vale anche per i gruppi non abeliani.

Definizione 17.21 Sia n un numero intero positivo. Si dice *funzione di Eulero* (o *funzione totiente*) di n il numero

$$\varphi(n) = |\mathcal{U}(\mathbb{Z}_n)|.$$

Alla luce della Proposizione 8.7, tale numero si può definire, equivalentemente, nel modo che segue:

$$\varphi(n) = \left|\{a \in \mathbb{Z} \mid 0 \le a \le n-1,\ a \text{ è coprimo con } n\}\right|.$$

Teorema 17.22 *(Teorema di Eulero)* Sia n un numero intero positivo. Allora, per ogni intero a tale che $\mathrm{MCD}(a, n) = 1$,

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Dimostrazione: Sia a un intero tale che $\mathrm{MCD}(a, n) = 1$. Allora, in base alla Proposizione 8.7, $[a]_n \in \mathcal{U}(\mathbb{Z}_n)$. Quindi, in base al Teorema di Lagrange, $o([a]_n)$ divide $\varphi(n)$. Pertanto, in base alla Proposizione 17.16,

$$[a]_n^{\varphi(n)} = [1]_n,$$

ove il primo membro è uguale a $[a^{\varphi(n)}]_n$. Segue la tesi. □

Teorema 17.23 *(Piccolo Teorema di Fermat)* Sia p un numero primo positivo. Allora, per ogni intero a,

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

Dimostrazione: Sia a un numero intero. Se p divide a, allora p divide anche a^p, e quindi $a^p \equiv a \equiv 0 \pmod{p}$. Supponiamo ora che p non divida a. Allora $\mathrm{MCD}(a, p) = 1$, e dunque, per il Teorema di Eulero, $a^{\varphi(p)} \equiv 1 \pmod{p}$. Ma, in base alla Proposizione 8.9, $\mathbb{Z}_p$ è un campo, e, di

conseguenza, $\mathcal{U}(\mathbb{Z}_p) = \mathbb{Z}_p \setminus \{[0]_p\}$. Pertanto $\varphi(p) = p-1$. Quindi $a^{p-1} \equiv 1 \pmod{p}$. Moltiplicando entrambi i membri per a, in base alla compatibilità della congruenza modulo p rispetto al prodotto (Proposizione 8.6 (ii)) si ottiene la tesi. □

Dedichiamo il resto di questa lezione ad una particolare classe di gruppi abeliani a cui, come vedremo, appartengono molti degli esempi da noi considerati in precedenza. I gruppi di questa classe sono ottenuti tramite una costruzione che consente di trovare, per un gruppo assegnato, molti dei suoi sottogruppi.

Proposizione 17.24 *(Sottogruppi ciclici)* Sia $(G,+)$ un gruppo additivo. Sia g un suo elemento. Allora

$$\langle g \rangle = \{ng \mid n \in \mathbb{Z}\}$$

è un sottogruppo abeliano di G.

(Sia $(G,\cdot)$ un gruppo moltiplicativo. Sia g un suo elemento. Allora

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$$

è un sottogruppo abeliano di G.)

Inoltre, ogni sottogruppo di G a cui appartiene g contiene $\langle g \rangle$. (Rispetto alla relazione di inclusione tra sottogruppi, $\langle g \rangle$ è il più piccolo sottogruppo di G a cui g appartenga.)

Dimostrazione: (Caso moltiplicativo) In base alla Definizione 17.1, $g^0 = 1_G \in \langle g \rangle$, quindi $\langle g \rangle \neq \varnothing$. Inoltre, per ogni $n,m \in \mathbb{Z}$, $g^n (g^m)^{-1} = g^n g^{-m} = g^{n-m} \in \langle g \rangle$, ove abbiamo utilizzato, nell'ordine, le parti (a) e (c) (i) della Proposizione 17.6. Ciò, in base alla caratterizzazione dei sottogruppi (Proposizione 2.24), prova che $\langle g \rangle$ è un sottogruppo di G. Inoltre, in base alla Proposizione 17.6 (c) (ii), per ogni $n,m \in \mathbb{Z}$, $g^n g^m = g^{n+m} = g^{m+n} = g^m g^n$. Ciò prova che $\langle g \rangle$ è un gruppo abeliano.
Per dimostrare l'ultima parte dell'enunciato, consideriamo un sottogruppo H di G tale che $g \in H$. Allora, in base alla Proposizione 2.21 (a), $1_G = g^0 \in H$. Inoltre, essendo H, per definizione, chiuso rispetto al prodotto di G, per ogni intero positivo n si ha $g^n \in H$. Alla luce della Proposizione 2.21 (b), ne consegue che, per ogni intero negativo n, $g^n = \left(g^{-n}\right)^{-1} \in H$. □

Definizione 17.25 Il gruppo $\langle g \rangle$ è detto *sottogruppo ciclico* di G *generato da* g. Se $G = \langle g \rangle$, il gruppo G si dice *ciclico.*

Esempio 17.26 (a) In base alla Proposizione 17.3 (b) e alla Proposizione 17.6 (b), il sottogruppo ciclico generato dall'elemento neutro è il sottogruppo banale.
(b) Per ogni $h \in \mathbb{Z}$, il sottogruppo ciclico generato da h è

$$\langle h \rangle = \{nh \mid n \in \mathbb{Z}\},$$

che coincide con l'insieme dei multipli del numero *h*, e per questo motivo viene solitamente indicato con $h\mathbb{Z}$. In particolare si ha $\langle 0\rangle = \{0\}$, $\langle 1\rangle = \mathbb{Z}$.

(c) Nel gruppo $(\mathbb{Z}_m, +)$, si ha $\langle [1]_m \rangle = \{a[1]_m \,|\, a \in \mathbb{Z}\} = \{[a]_m \,|\, a \in \mathbb{Z}\} = \mathbb{Z}_m$, quindi $\mathbb{Z}_m$ è un gruppo ciclico generato da $[1]_m$. (Per la seconda uguaglianza, si veda, più avanti, l'Esercizio 17.33).

Del prossimo enunciato diamo, per semplicità, soltanto la versione additiva.

Teorema 17.27 *(Caratterizzazione dei gruppi ciclici)* $(G,+)$ un gruppo additivo. Sia *g* un suo elemento.

a) Sia *g* aperiodico. Allora l'applicazione $\varphi : \mathbb{Z} \to \langle g \rangle$ definita, per ogni $a \in \mathbb{Z}$, da $\varphi(a) = ag$, è un isomorfismo di gruppi.

b) Sia *g* periodico di periodo *m*. Allora l'applicazione $\varphi : \mathbb{Z}_m \to \langle g \rangle$ definita, per ogni $a \in \mathbb{Z}$, da $\varphi([a]_m) = ag$, è un isomorfismo di gruppi.

Dimostrazione: a) L'applicazione φ è suriettiva per definizione. Inoltre, in base alla Proposizione 17.3 (c) (i), per ogni $a, b \in \mathbb{Z}$,

$$\varphi(a+b) = (a+b)g = ag + bg = \varphi(a) + \varphi(b),$$

il che prova che φ è un omomorfismo di gruppi. Infine, essendo *g* aperiodico, per ogni $a \in \mathbb{Z}$ si ha che $a \in \operatorname{Ker}\varphi \Rightarrow ag = 0 \Rightarrow a = 0$, quindi $\operatorname{Ker}\varphi = \{0\}$. Ciò prova che l'omomorfismo φ è anche iniettivo, e quindi è un isomorfismo.

b) Proviamo anzitutto che l'applicazione φ è ben definita. Siano $a, a' \in \mathbb{Z}$ tali che $[a]_m = [a']_m$. Allora *m* divide $a - a'$. Quindi, in base al Corollario 17.17, $\varphi(a) = ag = a'g = \varphi(a')$.

Come in a), si vede facilmente che φ è un omomorfismo suriettivo. Inoltre, in base alla Proposizione 17.16, per ogni $a \in \mathbb{Z}$ si ha che $[a]_m \in \operatorname{Ker}\varphi \Leftrightarrow ag = 0 \Leftrightarrow m$ divide $a \Leftrightarrow [a]_m = [0]_m$. Ciò prova che $\operatorname{Ker}\varphi = \{[0]_m\}$, e quindi l'omomorfismo φ è anche iniettivo. Pertanto è un isomorfismo. □

Il precedente teorema stabilisce che i gruppi ciclici sono, essenzialmente, di due tipi, come precisato nel seguente

Corollario 17.28

(a) Ogni gruppo ciclico generato da un elemento aperiodico è isomorfo a $(\mathbb{Z}, +)$;

(b) Ogni gruppo ciclico generato da un elemento periodico di periodo *m* è isomorfo a $(\mathbb{Z}_m, +)$.

Osservazione 17.29 Dall'enunciato (a) del Corollario 17.28 segue che ogni elemento di un gruppo finito è periodico. L'enunciato (b) del Corollario 17.28 si può precisare come segue. In base al Teorema 17.27 b), se *g* è un elemento periodico di $(G,+)$ ed ha periodo *m*, allora $\langle g \rangle = \varphi(\mathbb{Z}_m) = \{\varphi([0]_m), \varphi([1]_m), \varphi([2]_m) ..., \varphi([m-1]_m)\}$. Quindi

$$\langle g \rangle = \{0_G, g, 2g, ..., (m-1)g\}.$$

Nel caso moltiplicativo si ha, dunque, $\langle g \rangle = \{1_G, g, g^2, ..., g^{m-1}\}$.

Pertanto, un elemento periodico genera un gruppo di *ordine* pari a $o(g)$. Ciò spiega la notazione usata per indicare il periodo di *g* (che alcuni autori chiamano l'*ordine* di *g*).

Esercizio 17.30 Determinare il sottogruppo $\langle [2]_5 \rangle$ di $\mathcal{U}(\mathbb{Z}_5)$.

Svolgimento: Determiniamo, anzitutto, il periodo di $[2]_5$, ossia il più piccolo esponente positivo *n* tale che $[2]_5^{\,n} = [1]_5$. Si ha

$$[2]_5^{\,2} = [4]_5 \neq [1]_5, \quad [2]_5^{\,3} = [8]_5 = [3]_5 \neq [1]_5, \quad [2]_5^{\,4} = [16]_5 = [1]_5.$$

Segue che $o([2]_5) = 4$. Pertanto

$$\langle [2]_5 \rangle = \{[1]_5, [2]_5, [4]_5, [3]_5\} = \mathcal{U}(\mathbb{Z}_5).$$

Proposizione 17.31 *(Isomorfismo e ciclicità)* Siano G_1 e G_2 gruppi isomorfi. Allora, se G_1 è ciclico, anche G_2 è ciclico. Precisamente, se $G_1 = \langle g \rangle$ e $\varphi : G_1 \to G_2$ è un isomorfismo di gruppi, allora $G_2 = \langle \varphi(g) \rangle$.

Dimostrazione: Utilizziamo la notazione moltiplicativa. Essendo φ suriettivo, si ha

$$G_2 = \varphi(G_1) = \{\varphi(g^n) \,|\, n \in \mathbb{Z}\} = \{\varphi(g)^n \,|\, n \in \mathbb{Z}\} = \langle \varphi(g) \rangle.$$

La terza uguaglianza è dovuta al fatto che un omomorfismo tra gruppi moltiplicativi, conservando l'elemento neutro, i prodotti e gli inversi (v. Proposizione 3.3), conserva, alla luce della Definizione 17.4, anche le potenze. □

Esercizio 17.32 Dire se i gruppi additivi $\mathbb{Z}_4$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$ sono isomorfi.

Dimostrazione: In base alla Proposizione 17.31 ed al Corollario 17.28, un gruppo è isomorfo a $\mathbb{Z}_4$ se e solo se è ciclico di ordine 4 (ossia generato da un elemento di periodo 4). Però nessun elemento di $\mathbb{Z}_2 \times \mathbb{Z}_2$ ha periodo 4. Infatti l'elemento neutro, che è $([0]_2, [0]_2)$, ha periodo 1, mentre per i restanti elementi vale quanto segue:

$$2([0]_2, [1]_2) = 2([1]_2, [0]_2) = 2([1]_2, [1]_2) = ([0]_2, [0]_2).$$

Ciò prova che tali elementi hanno tutti periodo 2. Quindi $\mathbb{Z}_4$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$, pur avendo entrambi ordine 4, non sono gruppi isomorfi.

Esercizio 17.33* Sia *n* un intero positivo e siano *a*, *b* interi. Provare che $a[b]_n = [ab]_n$. (Questa proprietà è stata utilizzata negli Esempi 17.7 (b) e 17.26 (c)).

Esercizio 17.34* Sia *G* un gruppo moltiplicativo. Siano $g, h \in G$ tali che $gh = hg$. Provare che allora per ogni $n, m \in \mathbb{Z}$, $g^n h^m = h^m g^n$.

Proposizione 17.35 *(Ciclicità dei sottogruppi)* Ogni sottogruppo di un gruppo ciclico è ciclico.

Dimostrazione: Sia G un gruppo moltiplicativo ciclico, generato dall'elemento g. Sia H un sottogruppo di G. Se H è il sottogruppo banale, allora è ciclico, generato dall'elemento neutro di G. Altrimenti l'insieme $\{n \in \mathbb{Z}, n > 0 \mid g^n \in H\}$ è non vuoto (perché?). Sia t il suo minimo. Sia $h \in H$. Allora esiste un intero s tale che $h = g^s$. Siano q ed r il quoziente ed il resto della divisione euclidea di s per t. Allora $g^s = \left(g^t\right)^q g^r$, da cui $g^r = (g^t)^{-q} g^s \in H$. Poiché $0 \le r < t$, dalla minimalità di t segue che $r = 0$, ossia $g^s = \left(g^t\right)^q$. Ciò prova che $H \subset \langle g^t \rangle$. Ma vale anche l'inclusione opposta. Quindi $H = \langle g^t \rangle$. □

Lemma 17.36 *(Formula del periodo)* Sia G un gruppo moltiplicativo, e sia g un suo elemento periodico. Allora, per ogni intero k, l'elemento g^k è periodico e

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

Dimostrazione: L'elemento g^k è periodico in virtù del Teorema di Lagrange (Teorema 17.19), in quanto appartenente a $\langle g \rangle$, che è un gruppo abeliano finito. Posto $d = \mathrm{MCD}(o(g), k)$, siano r, s interi tali che $o(g) = rd$, $k = sd$. Allora, in base al Corollario 6.25, i numeri r e s sono coprimi. Sia ora n un intero. Allora, in base alla Proposizione 17.16, si ha $\left(g^k\right)^n = g^{kn} = 1_G$ se e solo se $o(g)$ divide kn, ossia se e solo se rd divide sdn, se e solo se r divide sn. Alla luce della Proposizione 6.24, ciò vale se e solo se r divide n. Il più piccolo intero positivo n verificante questa condizione è r, che, per definizione, è uguale a $\frac{o(g)}{\mathrm{MCD}(o(g), k)}$. Questo è dunque il periodo di g^k. □

Corollario 17.37 Un gruppo ciclico finito di ordine n possiede esattamente $\varphi(n)$ generatori.

Dimostrazione: Sia G un gruppo moltiplicativo finito. di ordine n, generato dall'elemento g, così che $o(g) = n$. In base all'Osservazione 17.29, $G = \{g^k \mid 0 \le k \le n-1\}$. Sia k un intero tale che $0 \le k \le n-1$. L'elemento g^k è un generatore di G se e solo se il suo periodo è n. Ora, secondo il Lemma 17.36, si ha $o(g^k) = n$ se e solo se $\mathrm{MCD}(n, k) = 1$. Il numero dei valori di k verificanti tale condizione, in base alla Definizione 17.21, è pari a $\varphi(n)$. □

Esempio 17.38 Riportando alla notazione moltiplicativa quanto stabilito nel corso della dimostrazione del precedente corollario, si vede che i generatori del gruppo ciclico $\mathbb{Z}_n (= \langle [1]_n \rangle)$ sono tutti e soli gli elementi $[a]_n (= a[1]_n)$, ove a è un intero tale che $0 \le a \le n-1$ ed a è coprimo con n. In altri termini, alla luce della Proposizione 8.7, i generatori del gruppo additivo $\mathbb{Z}_n$ sono tutti e soli gli elementi del gruppo delle unità dell'anello $\mathbb{Z}_n$.

Proposizione 17.39 *(Sottogruppi di un gruppo ciclico finito)*. Sia G un gruppo ciclico finito di ordine n. Allora, per ogni intero positivo d che divide n esiste uno ed un solo sottogruppo di G avente ordine d.

Dimostrazione: Sia G moltiplicativo, e sia g un suo generatore, di modo che $o(g)=n$. Sia d un intero positivo che divide n. Allora, in base al Lemma 17.36, si ha

$$o\left(g^{\frac{n}{d}}\right)=\frac{n}{\mathrm{MCD}\left(n,\frac{n}{d}\right)}=\frac{n}{\frac{n}{d}}=d,$$

e quindi $H=\left\langle g^{\frac{n}{d}}\right\rangle$ è un sottogruppo di G avente ordine d. Sia ora K un sottogruppo di G avente ordine d. In base alla Proposizione 17.35, K è allora un gruppo ciclico, esiste dunque un intero s tale che $K=\langle g^s\rangle$. In virtù del Lemma 17.36, si ha allora che $\mathrm{MCD}(n,s)=\frac{n}{d}$. In particolare $\frac{n}{d}$ divide s. Alla luce della Proposizione 9.2, ciò implica che la congruenza lineare $\frac{n}{d}x\equiv s \pmod{n}$ ha soluzione. Detta q una soluzione, in base al Corollario 17.17 si ha allora $g^s=g^{\frac{n}{d}q}=\left(g^{\frac{n}{d}}\right)^q\in H$. Ne consegue che $K=\langle g^s\rangle\subset H$. Poiché H e K hanno entrambi ordine d, si ha dunque $H=K$. Ciò prova l'unicità del sottogruppo di ordine d. □

Da quanto precede possiamo dedurre un'importante identità aritmetica riguardante la funzione di Eulero.

Corollario 17.40 *(Decomposizione di un intero positivo)* Sia n un intero positivo. Allora $\sum_{d|n}\varphi(d)=n$.

Dimostrazione: Sia G un gruppo ciclico di ordine n (certamente esistente). Ogni elemento di G genera un sottogruppo ciclico di G, il cui ordine è pari al periodo dell'elemento, ed è dunque un divisore di n in virtù del Teorema 17.19. Viceversa, dato un intero positivo d che divide n, sappiamo che esiste un elemento di G avente periodo d, che genera dunque un sottogruppo ciclico di G avente ordine d. Questo, in base alla Proposizione 17.39, è l'unico sottogruppo di G avente ordine d e, secondo il Corollario 17.37, ammette esattamente $\varphi(d)$ generatori. Dunque $\varphi(d)$ è il numero di elementi di G aventi periodo d. La tesi si ottiene allora contando gli elementi di G dopo averli raggruppati in base al periodo. □

Il prossimo enunciato ci fornisce un'ampia e significativa classe di gruppi ciclici.

Proposizione 17.41 *(Sottogruppi finiti del gruppo moltiplicativo di un campo)*. Ogni sottogruppo finito del gruppo moltiplicativo di un campo è ciclico.

Dimostrazione: Sia K un campo, e sia H un sottogruppo finito, di ordine n, del gruppo moltiplicativo K^*. Allora, in base al Teorema 17.19, ogni elemento di H è periodico ed ha come periodo un divisore di n. Dunque ogni elemento di H è radice del polinomio $f(X)=X^n-1$ a coefficienti in K. Poiché, in base al Corollario 12.15, $f(X)$ ha in K al più n radici (contate con le rispettive molteplicità), gli elementi di H sono le n radici (a due a due distinte) di $f(X)$ in K. Per ogni intero positivo d che divide n, sia H_d l'insieme delle radici in K del polinomio X^d-1. Poiché

questo polinomio è un divisore di $f(X)$, esso ammette d radici distinte. Inoltre H_d è un sottogruppo di H, ed ha ordine d. Ad esso appartengono tutti gli elementi di H aventi periodo d. Sia $\psi(d)$ il loro numero. Se $\psi(d) \neq 0$, H_d è un gruppo ciclico, ed in tal caso, in base al Corollario 17.37, $\psi(d) = \varphi(d)$. Tenendo conto del Corollario 17.40 se ne deduce che

$$n = \sum_{d|n} \psi(d) \leq \sum_{d|n} \varphi(d) = n.$$

Segue che la disuguaglianza centrale è un'uguaglianza. Ma ciò non sarebbe vero se, per qualche d, fosse $\psi(d) = 0$. Pertanto, in particolare, $\psi(n) \neq 0$, ossia H ammette un elemento di periodo n. Ciò prova che H è ciclico. □

Dalla precedente proposizione segue immediatamente:

Corollario 17.42 Per ogni numero primo $p > 0$, il gruppo delle unità dell'anello $\mathbb{Z}_p$ è ciclico.

Diamo infine un'ulteriore importante proprietà della funzione di Eulero, che ne agevola il calcolo.

Esercizio 17.43*

(a) Provare che, se $n_1, ..., n_s$ sono interi maggiori di 1 a due a due coprimi, allora

$$\varphi\left(\prod_{i=1}^{s} n_i\right) = \prod_{i=1}^{s} \varphi(n_i).$$

(b) Siano $p_1, ..., p_s$ numeri primi positivi, a due a due distinti, e siano $a_1, ..., a_s$ interi positivi. Provare che allora

$$\varphi\left(\prod_{i=1}^{s} p_i^{a_i}\right) = \prod_{i=1}^{s} p_i^{a_i - 1}(p_i - 1).$$

Concludiamo il capitolo ritornando alla struttura additiva di $\mathbb{Z}_n$.

Esercizio 17.44* Sia a un intero e sia A un anello unitario. Provare che, per ogni $x \in A$, $ax = (a1_A)x$.

Esercizio 17.45* Sia $n > 1$ un intero e sia A un anello unitario di cui $\mathbb{Z}_n$ è sottoanello. Supponiamo che $1_A \in \mathbb{Z}_n$. Provare che allora, per ogni $a \in \mathbb{Z}$,

$$a1_A = 0_A \Leftrightarrow n \text{ divide } a.$$

Dedurne che, per ogni $x \in A$ ed ogni $a \in \mathbb{Z}$ tale che n divide a, si ha $ax = 0_A$.

Provare inoltre che, se $n = p$ è primo, e A è commutativo, allora per ogni $x, y \in A$, $(x + y)^p = x^p + y^p$.