Gruppi, Caratteri e Teorema di Dirichlet (cenno)

Flaviano Battelli
Dipartimento di Ingegneria Industriale e Scienze Matematiche,
Università Politecnica delle Marche

1 Generalità

Sia $(G, \cdot)$ un gruppo con elemento neutro e. Ricordiamo che un sottogruppo di G, è un sottinsieme $H \subset G$ tale che $e \in H$ e $(H, \cdot)$ è un gruppo. Si può dimostrare che un sottinsieme non vuoto $H \subset G$ è un sottogruppo di G se e solo se per ogni coppia $x, y \in H$ risulta $xy^{-1} \in H$.[1] Se $H \subset G$ è un sottogruppo di G si scrive anche $H < G$.

Assegnato un sottogruppo di $H < G$ si può definire una relazione (in G) nel modo seguente:

$$g_1 \sim_H g_2 \Leftrightarrow g_2^{-1} g_1 \in H.$$

La relazione $\sim_H$ è una relazione di equivalenza. Infatti:

i) $g \sim_H g$ perché $g^{-1} g = e \in H$;

ii) se $g_1 \sim_H g_2$ risulta $g_2^{-1} g_1 \in H$, ma allora $g_1^{-1} g_2 = (g_2^{-1} g_1)^{-1} \in H \Rightarrow g_2 \sim_H g_1$.

iii) se $g_1 \sim_H g_2$ e $g_2 \sim_H g_3$ si ha $g_2^{-1} g_1 \in H$ e $g_3^{-1} g_2 \in H$. Moltiplicando otteniamo $g_3^{-1} g_1 = (g_3^{-1} g_2)(g_2^{-1} g_1) \in H$.

L'insieme $gH := \{gh \mid h \in H\}$ degli elementi di G che sono in relazione $\sim_H$ con $g \in G$ si dice *classe laterale sinistra* di H. Similmente potremmo definire un'altra relazione di equivalenza

$$g_1 {}_H\!\sim g_2 \Leftrightarrow g_2 g_1^{-1} \in H.$$

le cui classi di equivalenza sono gli insiemi $Hg := \{hg \mid h \in H\}$ detti *classi laterali destre* di H. In generale la classe laterale sinistra gH è diversa dalla destra Hg ma:

$$gH = Hg \text{ per ogni } g \in G, \text{ se e solo se } \sim_H = {}_H\!\sim .$$

Risulta utile definire anche gli insiemi

$$g_1 H g_2 = \{g_1 h g_2 \mid h \in H\}.$$

in particolare $g^{-1} H g = \{g^{-1} h g \mid h \in H\}$. Vale la seguente

[1] Infatti se H è un sottogruppo di G e $x, y \in H$ allora anche il reciproco y^{-1} di y appartiene ad H e quindi $xy^{-1} \in H$. Viceversa, se $x, y \in H \Rightarrow xy^{-1} \in H$ allora $e = x\,x^{-1} \in H$ (è necessario che esista almeno un $x \in H$ ossia che H sia non vuoto); se $x\,inH$ allora $e, x \in H \Rightarrow x{-}1 = x{-}1\,e \in H$ e se $x, y \in H \Rightarrow x, y^{-1} \in H \Rightarrow xy \in H$.

Proposizione 1.1. *Sia $H < G$. Le seguenti condizioni sono equivalenti.*

i) $\sim_H$ *è compatibile con l'operazione;*[2]

ii) per ogni $g \in G$ *risulta* $gH \subset Hg$*;*

iii) per ogni $g \in G$ *risulta* $gH = Hg$*;*

iv) per ogni $g \in G$ *risulta* $g^{-1}Hg \subset H$*;*

v) per ogni $g \in G$ *risulta* $g^{-1}Hg = H$*.*

Dimostrazione. Proviamo che *ii)* $\Leftrightarrow$ *iv)*. Siano $g \in G$ e $h \in H$. Da *ii)* segue che esiste $k \in H$ tale che $gh = kg$ e quindi $g^{-1}hg = k \in H$ il che prova *iv)*. Che *iv)* $\Rightarrow$ *ii)* si prova allo stesso modo. Similmente *iii)* $\Leftrightarrow$ *v)*. Proviamo che *ii)* $\Leftrightarrow$ *iii)*. Siano $g \in G$ e $h \in H$. Applicando *ii)* a $g^{-1} \in G$ e $h \in H$ si deduce che esiste $k \in H$ tale che $g^{-1}h = kg^{-1}$ ossia, moltiplicando a destra e a sinistra per g: $hg = gk$. Di conseguenza $Hg \subset gH$ e quindi *iii)*. Che *iii)* $\Rightarrow$ *ii)* è ovvio. Supponiamo ora che valga *i)* ossia che $\sim_H$ sia compatibile con l'operazione e siano $g \in G$ e $h \in H$. Dato che $h \sim_H e$ si ha (dalla compatibilità) $hg \sim_H g$ ossia esiste $k \in H$ tale che $g^{-1}hg = k \in H$. Di conseguenza vale *iv)*. Supponiamo ora che valga *iv)* e proviamo che $\sim_H$ è compatibile con l'operazione. Osserviamo, intanto, che $\sim_H$ è compatibile con la moltiplicazione a sinistra. Infatti se $g_1 \sim_H g_2$ e $g \in G$ risulta $(gg_2)^{-1}(gg_1) = g_2^{-1}g_1 \in H$ e quindi $gg_1 \sim_H gg_2$. Proviamo che nell'ipotesi *iv)* $\sim_H$ è compatibile con la moltiplicazione a destra. Infatti si ha $(g_2g)^{-1}(g_1g) = g^{-1}g_2^{-1}g_1g \in g^{-1}Hg \subset H$. Infine supponiamo che $g_1 \sim_H g_2$ e $\hat{g}_1 \sim_H \hat{g}_2$. Dalla compatibilità con la moltiplicazione a sinistra otteniamo

$$g_1\hat{g}_1 \sim_H g_1\hat{g}_2$$

mentre dalla compatibilità della moltiplicazione a destra:

$$g_1\hat{g}_2 \sim_H g_2\hat{g}_2$$

La conclusione segue dalla transitività della relazione d'equivalenza. □

Osservazione 1.1. *Dalla Proposizione 1.1 segue che* $\sim_H$ *è compatibile con l'operazione se e solo se* $\sim_H = {}_H\sim$.

Un sottogruppo $H < G$ si dice *normale*, e si scrive $H \triangleleft G$, se, per ogni $g \in G$, risulta $g^{-1}Hg = H$ ovvero se e solo se la relazione $\sim_H$ è compatibile con l'operazione. È chiaro che in un gruppo abeliano[3] tutti i sottogruppi sono normali.

Se $H \triangleleft G$ gli elementi di $G/\sim_H$ formano un gruppo detto *gruppo quoziente* che si indica con G/H. Gli elementi di G/H sono quindi le classi di equivalenza degli elementi di G modulo la relazione $\sim_H$. Se G/H è un gruppo finito il numero degli elementi di G/H si dice *indice di H in G* e si indica con $[G : H]$.

Sia $H < G$. Dato che la relazione $\sim_H$ è una relazione di equivalenza, le classi di equivalenza gH o coincidono o sono disgiunte. Dato che $g \in gH$ si ha $G = \bigcup_{g\in G} gH$ e quindi $|G| = \sum_{i\in I} |g_iH|$ dove gli elementi g_i sono tali che per ogni $i \neq j$ risulta $g_iH \cap g_jH = \emptyset$ e $G = \bigcup_{i\in I} g_iH$. L'insieme I è quindi in corrispondenza biunivoca con le classi di equivalenza di G modulo $\sim_H$ pertanto $|I| = [G : H]$. Questa formula non è molto interessante quando l'indice $[G : H]$ è infinito, ma lo è se $[G : H] < \infty$. Infatti è facile dimostrare che la funzione di $H \to gH$: $h \mapsto gh$ è una biiezione e quindi $|H| = |gH|$. Ma allora: *se $H < G$ e $[G : H] < \infty$, si ha*

$$|G| = [G : H]\,|H|.$$

Infatti è chiaro che la formula vale se $|H| = \infty$. Tuttavia è valida anche se $|H| < \infty$ ed in questo caso da $|G| = \sum_{i\in I} |g_iH|$ segue che $|G| < \infty$ e $|G| = [G : H]\,|H|$.

Chiamando *ordine di G* la cardinalità del gruppo G si ha ,come caso particolare:

[2] ossia se $g_1 \sim_H g_2$ e $\hat{g}_1 \sim_H \hat{g}_2$ risulta $g_1\hat{g}_1 \sim_H g_2\hat{g}_2$

[3] Un gruppo $(G, \cdot)$ si dice *abeliano o commutativo* se, per ogni $a, b \in G$ risulta $ab = ba$ (ossia se l'operazione è commutativa).

Proposizione 1.2. *L'ordine di un sottogruppo di un gruppo finito divide l'ordine del gruppo.*

Si noti che nel caso di gruppi finiti si ha $[G : H] = \frac{|G|}{|H|}$. La seguente proprietà dell'indice risulterà utile in seguito:

Proposizione 1.3. *Siano $H_1 \triangleleft H_2 \triangleleft G$ sottogruppi normali di un gruppo G. Allora*

$$[G : H_1] = [G : H_2][H_2 : H_1].$$

Dimostrazione. Se G è un gruppo finito la dimostrazione è immediata dato che $\frac{|G|}{|H_1|} = \frac{|G|}{|H_2|}\frac{|H_2|}{|H_1|}$. Nel caso generale si consideri l'omomorfismo (di gruppi finiti)[4] $\varphi : G/H_1 \to G/H_2$, $[g]_{H_1} \mapsto [g]_{H_2}$. Dato che $gH_1 \subset gH_2$ la definizione è ben posta. Inoltre $g \in \ker\varphi \Leftrightarrow [g]_{H_2} = H_2 \Leftrightarrow g \in H_2$ Quindi $\ker\varphi = H_2/H_1$. Dal Teorema di isomorfismo si ha:

$$G/H_1 \simeq \frac{(G/H_2)}{(H_2/H_1)}$$

e perciò $[G : H_1] = \frac{[G:H_2]}{[H_2:H_1]}$ ossia la tesi. □

2 Generatori e gruppi ciclici

Sia $(G, \cdot)$ un gruppo e $a \in G$ un suo elemento. Poniamo

$$a^0 = e, \quad a^1 = a.$$

Per ogni $n \in \mathbb{N}$, $n \geq 1$ poniamo poi: $a^{n+1} = a^n \cdot a$. Infine poniamo, per $n \in \mathbb{N}$: $a^{-n} = (a^{-1})^n$. In questo modo le potenze di a: a^n risultano definite per ogni $n \in \mathbb{Z}$. È semplice verificare che, per ogni $n, m \in \mathbb{Z}$, risulta

$$a^n \cdot a^m = a^{n+m}. \tag{1}$$

L'insieme $\{a^n \mid n \in \mathbb{Z}\}$ è quindi un sottogruppo di G, detto *sottogruppo ciclico generato da $a \in G$* e si indica con $< a >$. Se $H < G$ è un sottogruppo di G e $a \in H$ si ha $a^n \in H$ per ogni $n \in \mathbb{Z}$ e quindi $< a > \subset H$. Pertanto *ogni sottogruppo $H < G$ che contiene a contiene il sottogruppo generato da a.* In altre parole $< a >$ è il più piccolo sottogruppo di G che contiene a.

<u>*Esercizio*</u>. Provare[5] che per ogni $n, m \in \mathbb{Z}$ risulta $(a^n)^m = a^{nm}$. Di conseguenza: $(a^n)^m = (a^m)^n$.

In generale, sia $(G, \cdot)$ un gruppo e $\{G_\alpha\}_{\alpha\in A}$ una famiglia di sottogruppi di G. È facile verificare che $\bigcap_{\alpha\in A} G_\alpha$ è un sottogruppo di G (si osservi che $e \in G_\alpha$ per ogni α e quindi $e \in \bigcap_{\alpha\in A} G_\alpha \neq \emptyset$). Invece l'unione $\bigcup_{\alpha\in A} G_\alpha$ non è in generale un sottogruppo. Definiamo *somma dei gruppi* G_α il più piccolo sottogruppo di G (includendo G tra i sottogruppi di G) che contiene $\bigcup_{\alpha\in A} G_\alpha$. Questo sottogruppo si dice generato dai gruppi G_α e si indica con $< \bigcup_{\alpha\in A} G_\alpha >$. In pratica

$$\left\langle \bigcup_{\alpha\in A} G_\alpha \right\rangle = \bigcap_{\cup_{\alpha\in A} G_\alpha \subset H < G} H.$$

Si noti che tra i sottogruppi H di G tali che $\bigcup_{\alpha\in A} G_\alpha \subset H < G$ c'è certamente G.

Si ha la seguente

Proposizione 2.1. *Sia G un gruppo abeliano e $\{G_\alpha\}_\alpha$ una famiglia di sottogruppi di G. Allora $\langle \bigcup_{\alpha\in A} G_\alpha \rangle = \{g_1 \cdot \ldots \cdot g_n \mid g_i \in G_{\alpha_i},$ per qualche $\alpha_i \in A\}$.*

[4] Qui con $[g]_H$ si indica la classe di equivalenza di g modulo $\sim_H$.

[5] per induzione

Dimostrazione. Sia $\tilde{G} := \{g_1 \cdot \ldots \cdot g_n \mid g_i \in G_{\alpha_i}, \text{ per qualche } \alpha_i \in A\}$. Se $g_1 \cdot \ldots \cdot g_n$ e $g'_1 \cdot \ldots \cdot g'_m$ appartengono a $\tilde{G}$ si ha $(g_1 \cdot \ldots \cdot g_n) \cdot (g'_1 \cdot \ldots \cdot g'_m)^{-1} = g_1 \cdot \ldots \cdot g_n \cdot {g'_m}^{-1} \cdot \ldots \cdot {g'_1}^{-1} \in \tilde{G}$. D'altronde è chiaro che se $H < G$ è un sottogruppo di G che contiene tutti i sottogruppi G_α si ha anche $H \supset \tilde{G}$. □

Consideriamo il sottogruppo $< a >$ di G. Sono possibili soltanto due casi.

1 esiste $n \in \mathbb{N}$ tale che $a^n = e$

2 se $n, m \in \mathbb{Z}$, $n \neq m$ allora $a^n \neq a^m$.

Infatti se vale 1) allora $a^n = e = a^0$, $n > 0$, e quindi 2) è falsa. Se invece 2) non vale, possiamo supporre che $a^n = a^m$ con $m < n$. Allora moltiplicando l'uguaglianza $a^n = a^m$ per $a^{-m} = (a^{-1})^m$ si ottiene $a^{n-m} = e$ e $n - m \in \mathbb{N}$. □

Un gruppo G si dice *ciclico* se esiste $a \in G$ tale che $G =< a >$. Ovviamente un gruppo ciclico può essere finito o infinito. È finito se e solo se vale 1) mentre è infinito se e solo se vale 2). Nel caso che un gruppo ciclico $G =< a >$ sia infinito esiste un isomorfismo (non canonico) tra il gruppo $(\mathbb{Z}, +)$ e $(G, \cdot)$ dato da:

$$\mathbb{Z} \ni n \mapsto a^n \in G.$$

Il fatto che questo sia un omomorfismo deriva dalla (1), l'iniettività dall'alternativa *1 oppure 2 ma non entrambe* e la suriettività dalla definizione di $< a >$. Se invece vale 1 (ossia il gruppo è finito) l'applicazione precedente ha un nucleo. È immediato verificare che questo nucleo è il sottogruppo (additivo) di $(\mathbb{Z}, +)$ definito da $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$. Infatti se $m = nk$ si ha

$$a^m = (a^n)^k = 1.$$

Mentre se $a^m = 1$ dividendo m per n otteniamo $m = nq + r$, $q \in \mathbb{Z}$ e $0 \leq r < n$. Ma allora:

$$1 = a^m = a^{nq+r} = a^r \Rightarrow r = 0$$

e quindi $m = nq \in n\mathbb{Z}$. Dal teorema di isomorfismo dei gruppi otteniamo, per ogni *gruppo ciclico finito* di ordine n:

$$G \simeq \mathbb{Z}/(n\mathbb{Z}) = \mathbb{Z}_n$$

dove $\mathbb{Z}_n$ è il gruppo (additivo) delle classi resto $\mod n$. Questo gruppo si può definire utilizzando la relazione di equivalenza

$$x \equiv_n y \text{ se e solo se } n \text{ divide } x - y \tag{2}$$

ossia se e solo se esiste $k \in \mathbb{Z}$ tale che $x - y = kn$. Dato che $(\mathbb{Z}, +)$ è un gruppo abeliano si ha, per ogni $m \in \mathbb{Z}$: $m(nZ) = (mn\mathbb{Z} = \mathbb{Z}(mn) = (n\mathbb{Z})m$ e quindi la relazione (2) è compatibile con l'addizione $+$.

Supponiamo che valga 1) e sia $m \in \mathbb{Z}$. Dividendo m per n scriviamo $m = qn + r$ dove $0 \leq r < m$ e $q \in \mathbb{Z}$. Allora $a^m = a^{qn+r} = a^{qn}a^r = (1)^q a^r = a^r$. Quindi

$$< a >= \{e, a, a^2, \ldots, a^{n-1}\}.$$

D'altronde, se n è il più piccolo numero naturale per cui $a^n = e$ gli elementi $e, a, a^2, \ldots, a^{n-1}$ sono tutti diversi. Infatti se $a^h = a^k$, $0 \leq h < k \leq n - 1$ si avrebbe $a^{k-h} = e$, con $0 < k - h < n$. Il più piccolo numero naturale per i quale $a^n = e$ (se esiste), ossia l'ordine del gruppo $< a >$, si dice *ordine* o *periodo* di a. Ovviamente se G è un gruppo finito ogni elemento ha ordine finito e vale il seguente

Teorema 2.1. *Sia $(G, \cdot)$ un gruppo finito. Allora per ogni $a \in G$ l'ordine di a divide $|G|$.*

Dimostrazione. Dalla Proposizione 1.1 sappiamo che l'ordine del sottogruppo $< a >$ divide l'ordine di $|G|$ che è quanto si vuol dimostrare. □

Corollario 2.2. *Sia $(G,\cdot)$ un gruppo finito. Allora per ogni $a \in G$ risulta $a^{|G|} = 1$.*

Dimostrazione. Sia p l'ordine di a. Si ha $a^p = 1$ e, dal Teorema 2.1, sappiamo che p divide $|G|$ ossia $|G| = pq$ pr qualche $q \in \mathbb{N}$. Allora:

$$a^{|G|} = a^{pq} = (a^p)^q = 1^q = 1. \quad \square$$

Assegnati n gruppi $G_1, \ldots, G_n$ nell'insieme delle n-uple ordinate $(g_1, \ldots, g_n)$, con $g_i \in G_i$ si può introdurre un'operazione che rende $\mathcal{G} := G_1 \times \ldots \times G_n$ un gruppo. Questa operazione è definita da:

$$(g_1, \ldots, g_n) \cdot (\tilde{g}_1, \ldots, \tilde{g}_n) = (g_1\tilde{g}_1, \ldots, g_n\tilde{g}_n).$$

È chiaro che $(\mathcal{G},\cdot)$ è un gruppo in quanto evidentemente l'operazione è associativa, l'elemento neutro è $e = (e_1, \ldots, e_n)$ (dove e_i è l'elemento neutro di G_i) mentre l'inverso di $g := (g_1, \ldots, g_n)$ è $g^{-1} := (g_1^{-1}, \ldots, g_n^{-1})$.

Se $G_1, \ldots, G_n$ sono tutti sottogruppi di un assegnato gruppo G risulta anche definito il gruppo $G_1 + \ldots + G_n = < \bigcup_{i=1}^n G_i >$. Possiamo definire un'applicazione fra $\mathcal{G}$ e $G_1 + \ldots + G_n$ nel modo seguente:

$$\Phi : \mathcal{G} \to G_1 + \ldots + G_n,\ \Phi(g_1, \ldots, g_n) = g_1 \cdot \ldots \cdot g_n.$$

In generale Φ non è un omomorfismo dato che

$$\Phi[(g_1, \ldots, g_n) \cdot (\tilde{g}_1, \ldots, \tilde{g}_n)] = \Phi(g_1\tilde{g}_1, \ldots, g_n\tilde{g}_n) = g_1\tilde{g}_1 \cdot \ldots \cdot g_n\tilde{g}_n$$
$$\Phi(g_1, \ldots, g_n) \cdot \Phi(\tilde{g}_1, \ldots, \tilde{g}_n) = g_1 \cdot \ldots \cdot g_n \cdot \tilde{g}_1 \cdot \ldots \cdot \tilde{g}_n.$$

Tuttavia, se il gruppo G è abeliano si ha:

$$\Phi[(g_1, \ldots, g_n) \cdot (\tilde{g}_1, \ldots, \tilde{g}_n)] = \Phi(g_1, \ldots, g_n) \cdot \Phi(\tilde{g}_1, \ldots, \tilde{g}_n)$$

e quindi $\Phi : \mathcal{G} \to G_1 + \ldots + G_n$ è un omomorfismo di gruppi. Dato che G è abeliano, dalla Proposizione 2.1 segue che ogni elemento di $G_1 + \ldots + G_n$ è della forma $g_1 \cdot \ldots \cdot g_n$ dove $g_i \in G_i$. Ma allora ogni elemento di $G_1 + \ldots + G_n$ si scrive come $\Phi(g_1, \ldots, g_n)$, ossia Φ è suriettiva[6]. D'altronde $\ker\Phi = \{(g_1, \ldots, g_n) \mid g_1 \cdot \ldots \cdot g_n = e\}$ e questo può realizzarsi se e solo se per ogni i si ha

$$g_i = \Pi_{j \neq i} g_j^{-1} \tag{3}$$

D'altronde se l'eguaglianza (3) valesse per qualche $i \in \{1, \ldots, n\}$ allora $\Pi_{i=1}^n g_i = e$ e quindi per ogni $h \in \{1, \ldots, n\}$ risulterebbe $g_h = \Pi_{j \neq h} g_j^{-1}$. In pratica se la (3) vale per qualche $i \in \{1, \ldots, n\}$ allora vale per ogni $i \in \{1, \ldots, n\}$.

Ora se $\ker\Phi \neq \{(e, \ldots, e)\}$ (ossia $\ker\Phi$ contiene altri elementi oltre a $(e, \ldots, e)$, $e \in G$) scegliendo $(g_1, \ldots, g_n) \in \ker\Phi$, $(g_1, \ldots, g_n) \neq (e, \ldots, e)$ si avrà per qualche i $g_i \neq e$ e quindi dalla (3) dedurremo:

$$\{e\} \neq G_i \bigcap [G_1 + \ldots + G_{i-1} + G_{i+1} + \ldots + G_n].$$

D'altronde se esistesse i tale che $\{e\} \neq G_i \bigcap [G_1 + \ldots + G_{i-1} + G_{i+1} + \ldots + G_n]$, l'equazione (3) sarebbe soddisfatta da una n-upla $(g_1, \ldots, g_n) \in G_1 + \ldots + G_n$, con $(g_1, \ldots, g_n) \neq (e, \ldots, e)$ e quindi Φ non sarebbe iniettiva. Il risultato è il seguente:

Teorema 2.3. *Sia G un gruppo abeliano e siano $G_1, \ldots, G_n$ sottogruppi di G. Allora l'omomorfismo:*

$$\Phi(g_1, \ldots, g_n) = g_1 \cdot \ldots \cdot g_n$$

di $G_1 \times \ldots \times G_n$ in $G_1 + \ldots + G_n$ è un isomorfismo se e solo se per ogni $i \in \{1, \ldots, n\}$ risulta

$$G_i \cap \left[\bigcup_{j \neq i} G_j\right] = \{e\}. \tag{4}$$

[6] un omomorfismo suriettivo si dice anche *epimorfismo*

Se i sottogruppi $G_1, \ldots, G_n$ del gruppo abeliano G soddisfano la condizione (4) si dice che la somma $G_1 + \ldots + G_n$ è diretta e si scrive $G_1 \oplus \ldots \oplus G_n$.

Osservazione 2.4. *. Da quanto precede segue che $G_1 \oplus \ldots \oplus G_n$ se e solo se ogni elemento di $G_1 + \ldots + G_n$ si scrive in uno ed un solo modo come prodotto $g_1 \cdot \ldots \cdot g_n$ di elementi $g_i \in G_1$. Infatti se*

$$g_1 \cdot \ldots \cdot g_n = \tilde{g}_1 \cdot \ldots \cdot \tilde{g}_n$$

con $g_i \neq \tilde{g}_i$ per qualche i, risulta

$$g_1 \tilde{g}_1^{-1} \cdot \ldots \cdot g_n \tilde{g}_n^{-1} = e$$

e quindi $\{e\} \neq G_i \bigcap [G_1 + \ldots + G_{i-1} + G_{i+1} + \ldots + G_n]$. Viceversa se[7] $e \neq g_1 \in G_1 \bigcap [G_2 + \ldots + \ldots + G_n]$ allora

$$g_1 = g_2 \cdot \ldots \cdot g_n \Rightarrow e = g_1^{-1} g_2 \cdot \ldots \cdot g_n, \quad g_1^{-1} \neq e$$

e quindi e si scriverebbe in due modi diversi.

Esempio. Sia $G = \mathbb{R}^3$ con l'addizione fra vettori come operazione. Siano $G_1 = \{(x, 0, 0) \mid x \in \mathbb{R}\}$, $G_2 = \{(0, x, 0) \mid x \in \mathbb{R}\}$, $G_3 = \{(x, x, 0) \mid x \in \mathbb{R}\}$. Si ha $G_i \cap G_j = \{(0, 0, 0)\}$ per ogni $i \neq j$. Ma

$$G_3 \subset G_1 \oplus G_2$$

Quindi le condizioni $G_i \cap G_j = \{e\}$ non implicano, in generale, la (4).

Esercizio. Scrivere la tabella additiva del gruppo $(\mathbb{Z}_3 \times \mathbb{Z}_3, +)$.

3 Il monoide $(\mathbb{Z}_n, \cdot)$

La relazione (2) è compatibile anche con la moltiplicazione. Infatti se $a \equiv b$ e $\tilde{a} \equiv \tilde{b}$ $(a, b, \hat{a}, \hat{b} \in \mathbb{Z})$ si ha $n\tilde{n} \equiv m\tilde{m}$ dato che

$$a\tilde{a} - b\tilde{b} = a(\tilde{a} - \tilde{b}) + (a - b)\tilde{b}$$

è divisibile per n. Invece di scrivere $\equiv_m$ scriveremo anche "$\equiv \mod m$ cosicché

$$a \equiv_n b \Leftrightarrow a \equiv b \mod n \Leftrightarrow \ n \text{ divide } a - b.$$

Con l'operazione di moltiplicazione $\mathbb{Z}$ è un monoide[8] e l'insieme $\{a \in \mathbb{Z} \mid a \equiv_n 1\}$ è un sottomonoide moltiplicativo di[9] $(\mathbb{Z}, \cdot)$e quindi l'insieme delle classi resto $\mod n$ forma un monoide moltiplicativo[10] che indichiamo con $(\mathbb{Z}_n, \cdot)$. Si ha il seguente risultato

Teorema 3.1. *Sia $(M, \cdot)$ un monoide e G l'insieme degli elementi invertibili di M. Allora $(G, \cdot)$ è un gruppo.*

Dimostrazione. Se $x, y, z \in G$ si ha $(xy)z = x(yz)$ perchè l'uguaglianza vale in M. Dato che $e^{-1} = e$ risulta $e \in G$. Se $x, y \in G$ si ha anche $x^{-1}, y^{-1} \in G$ (x^{-1} e y^{-1} sono invertibili con inverso x e y rispettivamente) e $(xy)^{-1} = y^{-1}x^{-1}$. Quindi $xy \in G$. □

Osservazione 3.2. *Ovviamente ogni sottogruppo H di un monoide M è un sottogruppo del gruppo G degli elementi invertibili. Infatti se $x \in H$ allora x è invertibile e quindi appartiene a G.*

---

[7] Se $G_i \bigcap [G_1 + \ldots + G_{i-1} + G_{i+1} + \ldots + G_n]$ basta rinominare i gruppi in modo che $i = 1$.

[8] ricordiamo che un monoide è un insieme dotato di un'operazione associativa con elemento neutro.

[9] se $a = nh + 1$ e $b = nk + 1$ allora $ab = n(h + k + hk) + 1$ Si noti come questa sia essenzialmente la prova della compatibilità di $\equiv_n$ con la moltiplicazione.

[10] Esercizio: verificarlo

Indichiamo con $(\mathbb{Z}_n^*, \cdot)$ il gruppo degli elementi invertibili del monoide $(\mathbb{Z}_n, \cdot)$. Dal Teorema 3.1 segue che $(\mathbb{Z}_n^*, \cdot)$ è un gruppo moltiplicativo. L'ordine del gruppo $(\mathbb{Z}_n^*, \cdot)$ si indica con $\varphi(n)$. La funzione $\varphi : \mathbb{N} \to \mathbb{N}$, $n \mapsto \varphi(n)$ si chiama *funzione di Eulero*. Per ogni primo $p \in \mathbb{N}$ risulta $\varphi(p) = p - 1$ dato che i numeri naturali $1, \ldots, p-1$ sono tutti primi con p (in particolare $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$). Vale il seguente

Teorema 3.3 (Eulero)**.** *Per ogni $a \in \mathbb{Z}$ tale che* $\gcd(a, m) = 1$ *risulta* $a^{\varphi(m)} \equiv 1 \mod m$.

Dimostrazione Segue dal Corollario 2.2 in quanto, indicando con $\bar{a}$ la classe resto $\mod m$ di a, si ha $\bar{a} \in \mathbb{Z}_m^*$, e quindi per la compatibilità di $\equiv_m$ con la moltiplicazione (e perciò anche con l'elevamento a potenza):

$$a^{\varphi(m)} \equiv_m \bar{a}^{\varphi(m)} = \bar{a}^{|\mathbb{Z}_m^*|} \equiv_m 1$$

per il Corollario 2.2. □

Esempio. Dato che $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$ dal Teorema 3.3 segue $17^4 \equiv 1 \mod 12$. Verifichiamolo con un calcolo diretto:

$$17^4 \equiv 5^4 = (25)^2 \equiv 1^2 \equiv 1 \mod 12.$$

Corollario 3.4 (Fermat)**.** *Sia $p \in \mathbb{N}$ un numero primo. Allora $a^{p-1} \equiv 1 \mod p$.*

Dimostrazione. Segue da $\varphi(p) = p - 1$. □

Una conseguenza del Corollario 3.4 è il seguente *test di primalità*: Se esiste $a \in \{1, \ldots, n-1\}$ tale che $a^{n-1} \not\equiv 1 \mod n$ allora n non è primo.
Esempio. Verifichiamo se 1457 è primo calcolando 31^{1456}. Scriviamo 1456 in base 2. Si ha $1456 = 91 \cdot 2^4 = 90 \cdot 2^4 + 2^4 = 45 \cdot 2^5 + 2^4 = 44 \cdot 2^5 + 2^5 + 2^4 = 11 \cdot 2^7 + 2^5 + 2^4 = 10 \cdot 2^7 + 2^7 + 2^5 + 2^4 = 5 \cdot 2^8 + 2^7 + 2^5 + 2^4 = 2^{10} + 2^8 + 2^7 + 2^5 + 2^4$. Quindi:

$$31^{1456} = 31^{2^{10}+2^8+2^7+2^5+2^4} = 31^{2^{10}} \cdot 31^{2^8} \cdot 31^{2^7} \cdot 31^{2^5} \cdot 31^{2^4}.$$

Prima di procedere osserviamo che

$$a^{2^{n+1}} = \left(a^{2^n}\right)^2$$

Quindi otteniamo (le congruenze sono $\mod 1457$):

$$\begin{aligned}
&31^2 = 961 \equiv -496 \mod 1457\\
&31^{2^2} \equiv (-496)^2 = (496)^2 = 246016 \equiv -217\\
&31^{2^3} \equiv (-217)^2 = (217)^2 = 47089 \equiv 465\\
&31^{2^4} \equiv (465)^2 = 216225 \equiv 589\\
&31^{2^5} \equiv (589)^2 = 346921 \equiv 155\\
&31^{2^6} \equiv (155)^2 = 24025 \equiv 713\\
&31^{2^7} \equiv (713)^2 = 508369 \equiv 1333 \equiv -124\\
&31^{2^8} \equiv (-124)^2 = 15376 \equiv 806 \equiv -651\\
&31^{2^9} \equiv (-651)^2 = 423801 \equiv 1271 \equiv -186\\
&31^{2^{10}} \equiv (-186)^2 = 34596 \equiv 1085 \equiv -372
\end{aligned}$$

Quindi:

$$\begin{aligned}
&31^{1456} \equiv (-372)(-651)(-124)(155)(589) = -651(372 \cdot 124)(155 \cdot 589) = -651 \cdot 46128 \cdot 91295\\
&\equiv -651 \cdot 961 \cdot 961 \equiv -651 \cdot 496 \cdot 496 \equiv -651 \cdot (-217) = 1395 \equiv -62 \not\equiv 1 \mod 1457
\end{aligned}$$

Quindi 1457 non è primo (infatti $1457 = 31 \cdot 47$).

Teorema 3.5. *$a \in \mathbb{Z}_n^*$ se e solo se*[11] $\gcd(a,n) = 1$

La dimostrazione è conseguenza del seguente risultato:

Teorema 3.6 (Bézout)**.** *Siano $a, b \in \mathbb{Z}$, $a \neq 0 \neq b$. Allora* $\gcd(a,b) = \min\{ha+kb \mid h,k \in \mathbb{Z},\ ha+kb > 0\}$.

Dimostrazione (del Teorema di Bézout). Possiamo supporre che $a, b > 0$. Dato che $a = a \cdot 1 + b \cdot 0$ e $b = a \cdot 0 + b \cdot 1$ l'insieme $S = \{ha + kb \mid h, k \in \mathbb{Z},\ ha + kb > 0\}$ è non vuoto. Dunque esiste $d := \min S$ e si ha $d \leq a$ e $d \leq b$, inoltre esistono $\bar{h}, \bar{k} \in \mathbb{Z}$ tali che

$$d = \bar{h}a + \bar{k}b.$$

Proviamo che[12] $d \mid a$ e $d \mid b$. Dato che $d \leq a$ esistono $q, r \in \mathbb{N}$ tali che $a = dq + r$ con $0 \leq r < d$. Si ha $r = a - dq = a - (\bar{h}a + \bar{k}b)q = (1 - \bar{h}q)a + (-\bar{k}q)b$. Se fosse $r > 0$ si avrebbe dunque $r \in S$. Ma ciò è impossibile perché $d := \min S$. Quindi $r = 0$ e perciò $d \mid a$. Allo stesso modo si vede che $d \mid b$. Viceversa se $\hat{d} \mid a$ e $\hat{d} \mid b$ si ha $\hat{d} \mid \bar{h}a + \bar{k}b = d$ e quindi $d = \gcd(a,b)$. □

Corollario 3.7. [13] *Siano $a, b \in \mathbb{Z}$, $a \neq 0 \neq b$. Si ha* $\gcd(a,b) = 1$ *se e solo se esistono $h, k \in \mathbb{Z}$ tali che $ha + kb = 1$.*

Dimostrazione del Teorema 3.5. Supponiamo che $\gcd(a,n) = 1$. Dal Teorema di Bézout (o dal suo Corollario) segue che esistono $h, k \in \mathbb{Z}$ tali che $ha + kn = 1$ e quindi $ah \equiv 1 \mod n$ ovvero $h = a^{-1} \mod n$. Viceversa se esiste $b \in \mathbb{Z}$ tale che $ab \equiv 1 \mod n$ significa che esiste $k \in \mathbb{Z}$ tale che $ab = kn + 1$ ovvero $ab - kn = 1$ da cui segue $\gcd(a,b) = 1$ per il (Corollario del) Teorema di Bézout. □

Altre conseguenze importanti del Teorema di Bézout sono i risultati seguenti.

Corollario 3.8. *Siano $a, b, c \in \mathbb{Z}$, Allora se* $\gcd(a,b) = 1$ *e $a \mid bc$ risulta $a \mid c$.*

Dimostrazione. Dal Teorema 3.6 segue l'esistenza di $h, k \in \mathbb{Z}$ tali che $ah + bk = 1$. Moltiplicando per c si ottiene:

$$c = ahc + cbk$$

Dato che $a \mid bc$ esiste $m \in \mathbb{Z}$ tale che $bc = am$ e quindi:

$$c = ahc + cbk = ahc + amk = a(hc + mk)$$

ossia $a \mid c$. □

Corollario 3.9. *Se* $\gcd(m,n) = 1$ *e $a \equiv 0 \mod n$, $a \equiv 0 \mod m$, allora $a \equiv 0 \mod mn$.*

Dimostrazione. Per ipotesi esistono h, k tali che $hm = a = kn$. Dato che $\gcd(m,n) = 1$ e $n \mid hm$ dal Corollario 3.8 segue che $n \mid h$ ossia $h = qn$. Pertanto $a = hm = qnm$ e quindi $a \equiv 0 \mod mn$. □

Osservazione 3.10. *Dimostrare, procedendo per induzione, che se $m_1, \ldots, m_n$ sono due a due relativamente primi (ossia* $\gcd(m_i, m_j) = 1$*) si ha*

$$a \equiv 0 \mod m_i \text{ per ogni } i = 1, \ldots, n \Leftrightarrow a \equiv 0 \mod m_1 \cdot \ldots \cdot m_n.$$

[11] gcd indica il massimo comun divisore. Dato che se $d \mid a$ e $d \mid b$ anche $-d \mid a$ e $-d \mid b$ si ha $\gcd(a,b) > 0$. Inoltre se $d \mid a$ allora $d \mid (-a)$, quindi nel calcolo di $\gcd(a,b)$ si può supporre $a, b > 0$.

[12] Il simbolo $n \mid m$ si legge *n divide m* e significa che esiste $k \in \mathbb{Z}$ tale che $m = kn$.

[13] La dimostrazione è lasciata per esercizio.

Consideriamo come esempio il gruppo $(\mathbb{Z}_8^*, \cdot)$. Per il Teorema 3.5 gli elementi invertibili di $\mathbb{Z}_8$ sono $\{1, 3, 5, 7\}$. La tabella di moltiplicazione di $\mathbb{Z}_8^*$ è

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Osserviamo che $a^2 = 1$, per ogni $a \in \mathbb{Z}_8^*$ ossia il periodo di ogni elemento di $\mathbb{Z}_8^*$ è 2. In particolare $\mathbb{Z}_8^*$ *non è ciclico*. Consideriamo invece $(\mathbb{Z}_9^*, \cdot)$. Si ha $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$ e la tabella di moltiplicazione è:

$\cdot$	1	2	4	5	7	8
1	1	2	4	5	5	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Notiamo che $\{1, 4, 7\}$ è un sottogruppo di $(\mathbb{Z}_9^*, \cdot)$. In particolare $4^3 \equiv 7^3 \equiv 1 \mod 9$. Ma $\mathbb{Z}_9^* =< 5 >$. Infatti sappiamo che l'ordine di un sottogruppo $< a >$ divide l'ordine del gruppo (Teorema 2.1) e quindi per ogni $a \in \mathbb{Z}_9^*$ se $a^q \equiv 1 \mod 9$ deve essere $q = 1, 2, 3, 6$. Ma

$$5^1 = 5, \quad 5^2 = 7, \quad 5^3 = 8$$

e quindi il periodo di 5 è 6, ossia $\mathbb{Z}_9^* =< 5 >$ è un gruppo ciclico e un suo generatore è 5.

<u>*Esercizio*</u>. Scrivere la tabella di moltiplicazione di $(\mathbb{Z}_{12}^*, \cdot)$. $(\mathbb{Z}_{12}^*, \cdot)$ è ciclico? Confrontare la tabella di moltiplicazione di $(\mathbb{Z}_8^*, \cdot)$ e $(\mathbb{Z}_{12}^*, \cdot)$. C'è qualche analogia?[14]

Sorge spontanea la domanda: *quali fra i gruppi* $(\mathbb{Z}_n^*, \cdot)$ *sono ciclici?* Di seguito daremo una condizione necessaria per la ciclicità. Questa condizione è anche sufficiente (quindi caratterizzeremo i valori di n per i quali i gruppi $(\mathbb{Z}_n^*, \cdot)$ sono ciclici) ma quest'ultima parte non la proveremo.

Premettiamo il seguente risultato.

Teorema 3.11 (Teorema Cinese dei resti)**.** *Siano* $m_1, \dots m_n \in \mathbb{N}$ *tali che* $\gcd(m_i, m_j) = 1$ *per ogni* $i \neq j$. *Allora comunque assegnati* n *interi* $a_1, \dots, a_n$ *esiste un intero* $x \in \mathbb{Z}$ *tale che*

$$x \equiv a_j \mod m_j$$

e x *è univocamente determinato* $\mod M = \Pi_{i=1}^n m_i$.

Dimostrazione. Procediamo per induzione su n. Se $n = 1$ non c'è nulla da dimostrare ($x = a_1$). Supponiamo $n = 2$. *Proviamo l'esistenza*. Dal teorema di Bézout sappiamo che esistono $h, k \in \mathbb{Z}$ tali che $hm_1 + km_2 = 1$. Moltiplicando per a_1 e a_2 otteniamo:

$$a_1hm_1 + a_1km_2 = a_1 \qquad a_2hm_1 + a_2km_2 = a_2.$$

Poniamo $x = a_1km_2 + a_2hm_1$. Si ha (scriviamo $\equiv_m$ per l'equivalenza $\mod m$):

$$x \equiv_{m_1} a_1km_2 = a_1(1 - hm_1) \equiv_{m_1} a_1$$

[14]Nella tabella di $(\mathbb{Z}_8^*, \cdot)$ scrivere 5 invece di 3, 7 invece di 5 e 11 invece di 7. Cosa si ottiene?

e

$$x \equiv_{m_2} a_2 h m_1 = a_2(1 - k m_2) \equiv_{m_2} a_2.$$

il che conclude la dimostrazione dell'esistenza. *Proviamo l'unicità.* Siano $x, y \in \mathbb{Z}$ tali che $x \equiv_{m_1} y \equiv_{m_1} a_1$ e $x \equiv_{m_2} y \equiv_{m_2} a_2$. Si ha $x - y \equiv_{m_1} 0$, $x - y \equiv_{m_2} 0$. Ossia esistono $h, k \in \mathbb{Z}$ tali che $x - y = hm_1$ e $x - y = km_2$. Quindi $hm_1 = km_2$. Dato che $\gcd(m_1, m_2) = 1$ dal Corollario 3.8 segue $m_1 \mid k$ ossia $k = cm_1$ per qualche $c \in \mathbb{Z}$. In conclusione: $x - y = km_2 = cm_1 m_2 \Rightarrow x - y \equiv 0 \mod m_1 m_2$.

Supponiamo ora che la tesi sia valida quando si considerano $n-1$ numeri interi primi fra loro e siano $m_1, \ldots, m_n$ come nelle ipotesi del Teorema. *Proviamo l'esistenza.* Se $m_n \mid m_1 \cdot \ldots \cdot m_{n-1}$, dato che $\gcd(m_n, m_{n-1}) = 1$ si avrebbe (Corollario 3.8) $m_n \mid m_1 \cdot \ldots \cdot m_{n-2}$. Così procedendo si arriverebbe a $m_n \mid m_1$ che contraddice l'ipotesi. Quindi $\gcd(m_n, m_1 \cdot \ldots \cdot m_{n-1}) = 1$. Per l'ipotesi di induzione esiste $\bar{x} \in \mathbb{Z}$ (univocamente determinato $\mod m_1 \cdot \ldots \cdot m_{n-1}$) tale che

$$\bar{x} \equiv a_i \mod m_i$$

per ogni $i = 1, \ldots, n-1$. Dato che $\gcd(m_n, m_1 \cdot \ldots \cdot m_{n-1}) = 1$ esiste $x \in \mathbb{Z}$ (univocamente determinato $\mod M = m_1 \cdot \ldots \cdot m_n$) tale che

$$x \equiv \bar{x} \mod m_1 \cdot \ldots \cdot m_{n-1} \qquad \text{e} \qquad x \equiv a_n \mod m_n.$$

Dato che $x - \bar{x} \equiv 0 \mod m_1 \cdot \ldots \cdot m_{n-1}$ e $m_i \mid m_1 \cdot \ldots \cdot m_{n-1}$ si ha anche $x - \bar{x} \equiv 0 \mod m_i$ per ogni $i \in \{1, \ldots, n-1\}$ e quindi $x \equiv a_i \mod m_i$ per ogni $i \in \{1, \ldots, n-1\}$. *Proviamo l'unicità.* Supponiamo che $x \equiv y \mod m_i$ per ogni $i = 1, \ldots, n$ ovvero $x - y \equiv 0 \mod m_i$. Dall'osservazione sucessiva al Corollario 3.9 otteniamo $x - y \equiv 0 \mod m_1 \cdot \ldots \cdot m_{n-1}$ e anche $x - y \equiv 0 \mod m_n$. Quindi

$$x - y = hm_1 \cdot \ldots \cdot m_{n-1} \text{ e } x - y = km_n.$$

Ma allora $hm_1 \cdot \ldots \cdot m_{n-1} = km_n$. Come nella parte precedente da ciò segue che $m_n \mid h$ e quindi $x - y \mid m_1 \cdot \ldots \cdot m_n$. □

Esercizi. Scrivere la tabella additiva del gruppo $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$[15] e confrontarla con quella moltiplicativa di $(\mathbb{Z}_8^*, \cdot)$. Provare che l'applicazione $\phi : (\mathbb{Z}_2 \times \mathbb{Z}_2, +) \to (\mathbb{Z}_8^*, \cdot)$ definita da

$$\phi(0,0) = 1, \quad \phi(0,1) = 3, \quad \phi(1,0) = 5, \quad \phi(1,1) = 7$$

è un isomorfismo di gruppi.[16]

ii) Scrivere la tavola dell'operazione nel gruppo $\mathbb{Z}_4^* \times \mathbb{Z}_2$ dove $(a, b) \odot (\tilde{a}, \tilde{b}) := (a\tilde{a}, b + \tilde{b})$. Confrontare la tavola con quella in $\mathbb{Z}_8^*$ cosa si può dire?

iii) Provare che $(\mathbb{Z}_4^*, \cdot) \simeq (\mathbb{Z}_2, +)$ e scrivere esplicitamente l'isomorfismo. Dedurre che $(\mathbb{Z}_8^*, \cdot) \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ e scrivere esplicitamente l'isomorfismo.

L'importanza del Teorema Cinese dei resti risulta più evidente ricorrendo al concetto di prodotto di gruppi. Siano $m_1, \ldots, m_n$ interi tali che $\gcd(m_i, m_j) = 1$ per ogni $i \neq j$.[17] Dal Teorema 3.11 deduciamo che per ogni n-upla $(a_1, \ldots, a_n) \in \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}$ esiste un unico $a \in \mathbb{Z}_m$, $m = m_1 \cdot \ldots \cdot m_n$ tale che $a \equiv a_i \mod m_i$, per ogni $i = 1, \ldots, n$. Poniamo

$$\Phi(a_1, \ldots, a_n) = a \in \mathbb{Z}_m$$

[15]La tabella additiva è

·	(0,0)	(1,0)	(0,1)	(1,1)
(0,0)	(0,0)	(1,0)	(0,1)	(1,1)
(1,0)	(1,0)	(0,0)	(1,1)	(0,1)
(0,1)	(0,1)	(1,1)	(0,0)	(1,0)
(1,1)	(1,1)	(0,1)	(1,0)	(0,0)

[16]Nella tabella di $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ sostituire $+$ con $\cdot$, $(0,0)$ con 1, $(1,0)$ con 3, $(0,1)$ con 5 e $(1,1)$ con 7. Cosa si ottiene?

[17]si dice che $m_1, \ldots, m_n$ sono *coprimi due a due.*

ossia $\Phi : \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n} \to \mathbb{Z}_m$ e

$$\Phi(a_1, \ldots, a_n) \equiv a_i \mod m_i. \tag{5}$$

Si ha il seguente

Teorema 3.12. *Siano $m_1, \ldots, m_n \in \mathbb{N}$ tali che $\gcd(m_i, m_j) = 1$ per ogni $i \neq j$. Poniamo $m = m_1 \cdot \ldots \cdot m_n$. Allora*

i) la funzione $\Phi : \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n} \to \mathbb{Z}_m$ definita dalla (5) è un isomorfismo di gruppi additivi;

ii) la funzione $\Phi : \mathbb{Z}_{m_1}^* \times \ldots \times \mathbb{Z}_{m_n}^* \to \mathbb{Z}_m^*$ definita dalla (5) è un isomorfismo di gruppi moltiplicativi.

Dimostrazione. (*Premessa*) Abbiamo già visto che la funzione $\Phi : \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n} \to \mathbb{Z}_m$, $\Phi(a_1, \ldots, a_n) = a$ dove $a \equiv a_i \mod m_i$ è ben definita. Proviamo che Φ è iniettiva. Se $\Phi(a_1, \ldots, a_n) = \Phi(\hat{a}_1, \ldots, \hat{a}_n) = a$ si ha, per ogni i, $a_i \equiv a \equiv \hat{a}_i \mod m_i$ e quindi $(a_1, \ldots, a_n) = (\hat{a}_1, \ldots, \hat{a}_n)$. Inoltre Φ è suriettiva dato che, ponendo a_i uguale al resto della divisione di a per m_i si ha $a \equiv a_i \mod m_i$ e quindi $a = \Phi(a_1, \ldots, a_n)$.

i) Proviamo che $\Phi : \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n} \to \mathbb{Z}_m$ è un omomorfismo (e quindi per la biiettività un isomorfismo) di gruppi additivi. Infatti, se $\Phi(a_1, \ldots, a_n) = a$ e $\Phi(b_1, \ldots, b_n) = b$ dalla compatibilità della relazione $\equiv_{m_i}$ con l'addizione segue $a + b \equiv a_i + b_i \mod m_i$ ossia $\Phi[(a_1, \ldots, a_n) + (b_1, \ldots, b_n)] = \Phi(a_1 + b_1, \ldots, a_n + b_n) = a + b = \Phi(a_1, \ldots, a_n) + \Phi(b_1, \ldots, b_n)$.

ii) Proviamo che $\Phi : \mathbb{Z}_{m_1}^* \times \ldots \times \mathbb{Z}_{m_n}^* \to \mathbb{Z}_m^*$ è un isomorfismo di gruppi moltiplicativi. Intanto, se $\Phi(a_1, \ldots, a_n) = a$ e $\Phi(b_1, \ldots, b_n) = b$, dalla compatibilità di $\equiv_m$ con la moltiplicazione si ha subito

$$\Phi[(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n)] = \Phi(a_1 b_1, \ldots, a_n b_n) = ab = \Phi(a_1, \ldots, a_n) \cdot \Phi(b_1, \ldots, b_n).$$

Inoltre, se $(a_1, \ldots, a_n) \in \mathbb{Z}_{m_1}^* \times \ldots \times \mathbb{Z}_{m_n}^*$ per il Teorema 3.5 esiste $(b_1, \ldots, b_n) \in \mathbb{Z}_{m_1}^* \times \ldots \times \mathbb{Z}_{m_n}^*$ tale che $a_i b_i \equiv 1 \mod m_i$. Posto $b = \Phi(b_1, \ldots, b_n)$ si ha $ab \equiv_{m_i} a_i b_i \equiv_{m_i} \equiv_{m_i} 1$ ossia $b \equiv a^{-1} \mod m$. Quindi $a \in \mathbb{Z}_m^*$ e Φ è un omomorfismo dei gruppi moltiplicativi $\mathbb{Z}_{m_1}^* \times \ldots \times \mathbb{Z}_{m_n}^*$ e $\mathbb{Z}_m^*$. L'iniettività di Φ è già stata dimostrata (non dipende dalla operazione considerata). Proviamo la suriettività. Se $a \in \mathbb{Z}_m^*$, esiste $b \in \mathbb{Z}_m^*$ tale che $ab \equiv_m 1$. Se a_i e b_i sono i resti della divisione per m_i di a e b rispettivamente si ha, per la compatibilità di $\equiv_m$ con la moltiplicazione, $ab \equiv a_i b_i \mod m_i$. Ciò significa che esiste $h \in \mathbb{Z}$ tale che $a_i b_i = ab + h m_i$ ma $ab \equiv 1 \mod m$ significa che $ab = 1 + km$ per qualche $k \in \mathbb{Z}$. In conclusione, ricordando che $m = m_1 \cdot \ldots \cdot m_n$: $a_i b_i \equiv 1 \mod m_i$ ossia $a_i \in \mathbb{Z}_{m_i}^*$. □

Corollario 3.13. *Sia $\varphi(m)$ la funzione di Eulero. Allora se $m = m_1 \cdot \ldots \cdot m_n$ con $\gcd(m_i, m_j) = 1$ per ogni $i \neq j$ si ha*

$$\varphi(m) = \varphi(m_1) \cdot \ldots \cdot \varphi(m_n). \tag{6}$$

Dimostrazione. Dato che $\varphi(m) = |\mathbb{Z}_m^*|$ la tesi segue direttamente dal punto ii) del Teorema 3.12 osservando che $|\mathbb{Z}_{m_1}^* \times \ldots \times \mathbb{Z}_{m_n}^*| = |\mathbb{Z}_{m_1}^*| \ldots |\mathbb{Z}_{m_n}^*|$. □

Esempi. i) Si ha $\mathbb{Z}_{12}^* \simeq \mathbb{Z}_3^* \times \mathbb{Z}_4^*$. Ora $\mathbb{Z}_3^* = \{1, 2\}$ e $\mathbb{Z}_4^* = \{1, 3\}$ e $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$. L'isomorfismo $\Phi : \mathbb{Z}_3^* \times \mathbb{Z}_4^* \to \mathbb{Z}_{12}^*$ del Teorema 3.12 è definito da:

$$\Phi : \begin{cases} (1,1) \mapsto 1 \\ (1,3) \mapsto 7 \\ (2,1) \mapsto 5 \\ (2,3) \mapsto 11 \end{cases}$$

In pratica è più semplice determinare Φ^{-1} Infatti, dalla dimostrazione del Teorema 3.12, sappiamo che $\Phi^{-1}(a) = (a_1, a_2)$ dove $a_i \equiv a \mod m_i$. Così, per esempio, $\Phi^{-1}(11) = (2, 3)$ perché $11 \equiv 2 \mod 3$ e $11 \equiv 3 \mod 4$. Osserviamo anche che essendo $\mathbb{Z}_{12}^*$ isomorfo al prodotto di due gruppi ciclici di ordine

2 ogni elemento di $\mathbb{Z}_{12}^*$ ha periodo 2, ossia $a^2 \equiv 1 \mod 12$ per ogni $a \in \mathbb{Z}$ tale che $\gcd(a, 12) = 1$. Si confronti questo risultato con il Teorema 3.3.

ii) Abbiamo visto che $\mathbb{Z}_8^* \simeq \mathbb{Z}_{12}^* \simeq \mathbb{Z}_3^* \times \mathbb{Z}_4^*$ e quindi non è vero che $\mathbb{Z}_8^* \simeq \mathbb{Z}_2^* \times \mathbb{Z}_2^* \times \mathbb{Z}_2^*$ (anche perché $\mathbb{Z}_2^* = \{1\}$). Costruire un isomorfismo fra $\mathbb{Z}_3^* \times \mathbb{Z}_4^*$ e $\mathbb{Z}_8^*$.

iii) Abbiamo visto che $(\mathbb{Z}_8^*, \cdot) \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$. Provare che $(\mathbb{Z}_{16}^*, \cdot) \not\simeq (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, +)$.[18]

Sia $m \in \mathbb{N}$. Dal teorema fondamentale dell'aritmetica possiamo scrivere $m = p_1^{k_1} \dots p_n^{k_n}$, dove $p_1, \dots, p_n$ sono primi distinti e $k_i > 0$. Dal Teorema 3.12 si ottiene:

$$\mathbb{Z}_m^* \simeq \times \mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_n^{k_n}}.$$

quindi (vedi anche il Corollario 3.13) $\varphi(m) = \varphi(p_1^{k_1}) \dots \varphi(p_n^{k_n})$. Ora per ogni numero primo p si ha $\varphi(p^k) = p^{k-1}(p-1)$, Infatti nell'insieme $\mathbb{Z}_{p^k} = \{0, 1, 2, \dots, p^k - 1\}$ i numeri che non sono coprimi con p^k sono solo quelli divisibili per p ossia i multipli di p e questi sono:

$$0 \cdot p, 1p, \dots (p^{k-1} - 1)p.$$

Pertanto

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1). \tag{7}$$

Otteniamo quindi:

$$\varphi(m) = \varphi(p_1^{k_1} \dots p_n^{k_n}) = p_1^{k_1 - 1} \dots p_n^{k_n - 1} \Pi_{i=1}^n (p_i - 1) = m \frac{\Pi_{i=1}^n (p_i - 1)}{\Pi_{i=1}^n p_i}. \tag{8}$$

Proposizione 3.1. *Se $(\mathbb{Z}_m^*, \cdot)$ è ciclico allora m è del tipo $2, 4, p^k, 2p^k$ con p primo dispari.*

Dimostrazione. Sia $m = p_1^{k_1} \dots p_n^{k_n}$, con $p_i \neq p_j$ per ogni $i \neq j$. Sia $q = \text{mcm}\{(p_1 - 1)p_1^{k_1 - 1}, \dots, (p_n - 1)p_n^{k_n - 1}\}$. Per il Teorema 3.12-ii) ogni elemento $a \in \mathbb{Z}_m^*$ si può scrivere $a = \Phi(a_1, \dots, a_n)$, $a_j \in \mathbb{Z}_{p_j}^*$. Quindi:

$$a^q = \Phi(a_1, \dots, a_n)^q = \Phi(a_1^q, \dots, a_n^q).$$

Ma l'ordine di $\mathbb{Z}_{p_j}^*$ divide q (essendo uguale a $(p_j - 1)p_j^{k_j - 1}$) e quindi (per il Corollario 2.2): $a_j^q = 1$. Ma allora:

$$a^q = \Phi(1, \dots, 1) = 1.$$

In conclusione l'odine di ogni elemento $a \in \mathbb{Z}_m^*$ divide $\text{mcm}\{(p_1 - 1)p_1^{k_1 - 1}, \dots, (p_n - 1)p_n^{k_n - 1}\}$.

Supponiamo allora che nella decomposizione di m in fattori primi ci siano almeno due primi dispari distinti, diciamo p_i e p_j, $i \neq j$. Dato che $2 \mid p_i - 1$ e $2 \mid p_j - 1$, $\text{mcm}\{(p_1 - 1)p_1^{k_1 - 1}, \dots, (p_n - 1)^{k_1 - 1}\}$ è un divisore proprio di $(p_1 - 1)p_1^{k_1 - 1} \cdot \dots \cdot (p_n - 1)^{k_1 - 1} = \varphi(m)$. Pertanto nessun elemento di $\mathbb{Z}_m^*$ ha periodo $\varphi(m) = |\mathbb{Z}_m^*|$. Di conseguenza $\mathbb{Z}_m^*$ non è ciclico. Supponiamo ora che $m = 2^h p^k$, con p primo dispari, $k \geq 1$ e $h \geq 2$. Ragionando come sopra vediamo che ogni elemento di $\mathbb{Z}_{2^h p^k}$ ha periodo $\text{mcm}\{2^{h-1}, (p-1)p^{k-1}\}$ che è un divisore proprio di $\varphi(2^h p^k) = 2^{h-1}(p-1)p^{k-1}$ dato che $2 \mid 2^{h-1}$ e $2 \mid (p-1)$. Quindi anche $\mathbb{Z}_{2^h p^k}^*$ non è ciclico se $h \geq 2$ e $k \geq 1$. Restano i casi $\mathbb{Z}_{p^k}^*$, $\mathbb{Z}_{2p^k}^*$ e $\mathbb{Z}_{2^k}^*$. È facile verificare che i gruppi moltiplicativi $\mathbb{Z}_2^* = \{1\}$ e $\mathbb{Z}_4^* = \{1, 3\}$ sono entrambi ciclici (il secondo con generatore 3). Consideriamo il gruppo $(\mathbb{Z}_{2^k}^*, \cdot)$ con $k > 2$. Proviamo che se $m = 2h + 1$ è un numero dispari si ha $m^{2^k} \equiv 1 \mod 2^{k+2}$. Procediamo per induzione. Se $k = 1$ si tratta di dimostrare che

$$(2h + 1)^2 \equiv 1 \mod 8.$$

[18] Ogni elemento del secondo gruppo ha periodo ..., vale lo stesso per il primo?

Ora $(2h+1)^2 = 4h(h+1)+1 \equiv 1 \mod 8$ perché uno fra h e $h+1$ è pari. Supponiamo di aver provato che per ogni $h \in \mathbb{Z}$ risulta $(2h+1)^{2^{k-1}} \equiv 1 \mod 2^{k+1}$ ossia $(2h+1)^{2^{k-1}} = 2^{k+1}n+1$ per qualche $n \in \mathbb{Z}$. Si ha:

$$(2h+1)^{2^k} = ((2h+1)^{2^{k-1}})^2 = (2^{k+1}n+1)^2 = 2^{2k+2}n^2 + 2^{k+2}n + 1 = 2^{k+2}n[2^k n+1]+1 \equiv 1 \mod 2^{k+2}.$$

Quindi, se $k > 2$ gli elementi di $(\mathbb{Z}_{2^k}^*, \cdot)$ hanno (un divisore di) 2^{k-2} come periodo. Ma $\mathbb{Z}_{2^k}^*$ ha 2^{k-1} elementi e quindi non è ciclico. □

Osservazione 3.14. *Si può dimostrare che i gruppi moltiplicativi $\mathbb{Z}_2^*, \mathbb{Z}_4^*, \mathbb{Z}_{p^k}^*$ e $\mathbb{Z}_{2p^k}^*$, con p primo dispari sono tutti ciclici. È chiaro che $\mathbb{Z}_2^* = \{1\}$ e $\mathbb{Z}_4^* = \{1,3\} = \langle 3 \rangle$ lo sono. Dal Teorema Cinese dei resti segue poi $\mathbb{Z}_{2p^k}^* \simeq \mathbb{Z}_2^* \times \mathbb{Z}_{p^k}^* \simeq \mathbb{Z}_{p^k}^*$. Quindi tutto si riduce a provare che, per ogni primo p, $\mathbb{Z}_{p^k}^*$ è ciclico.*

Esercizi. i) Scrivere la tabella moltiplicativa di $(\mathbb{Z}_{16}^*, \cdot)$e verificare che per ogni $a \in \mathbb{Z}_{16}^*$ risulta $a^4 \equiv 1 \mod 16$.

ii) Costruire un isomorfismo fra $(\mathbb{Z}_4 \times \mathbb{Z}_2, +)$ e $(\mathbb{Z}_{16}^*, \cdot)$.

iii) Determinare tutti i generatori di $(\mathbb{Z}_{10}^*, \cdot)$ e di $(\mathbb{Z}_{18}^*, \cdot)$.[19]

iv) Trovare un generatore di $\mathbb{Z}_{27}^*$ e uno di $\mathbb{Z}_{81}^*$

v) Per ogni divisore d di $\varphi(27)$ costruire un sottogruppo ciclico di $\mathbb{Z}_{27}^*$ di ordine d.

Osservazione 3.15. Il teorema di Eulero e la (7) vengono utilizzati nel metodo RSA[20] in crittografia. Il metodo funziona così. Supponiamo che l'utente A voglia trasmettere all'utente B un numero, per esempio 1234, e che non voglia che altri possano riconoscerlo durante la trasmissione. L'utente B forma due chiavi, una pubblica e una privata utilizzando due numeri primi grandi, per esempio[21] 23 e 31, e chiama n il loro prodotto (nell'esempio $23 \cdot 31 = 713$). Calcoliamo $\varphi(713) = \varphi(23 \cdot 31) = 22 * 30 = 660$. Osserviamo che il calcolo di $\phi(713)$ è reso semplice dalla fattorizzazione di 713 in numeri primi. Non conoscendo questa decomposizione il calcolo avrebbe preso molto più tempo.[22] B sceglie ora un numero e primo con $\varphi(n)$ e calcola il suo inverso $\mod \varphi(n)$. La ricerca si può fare fattorizzando uno dei numeri $1 + k\varphi(n)$, $k \in \mathbb{N}$. Nell'esempio considerato si ha:

$$1 + 660 = 661 (\text{non va: è primo})$$
$$1 + 2 \cdot 660 = 1321 (\text{non va: è primo})$$
$$1 + 3 \cdot 660 = 1981 = 7 \cdot 283$$

Quindi B sceglie $e = 7$, $f = 283$. La *chiave pubblica* è la coppia $(e, n) = (7, 713)$ quella privata è $(f, n) = (283, 713)$. Ora A trasmette il numero 1234 a B utilizzando la chiave pubblica di B. Il metodo consiste nel trasmettere $a^f \mod n$ invece di a. Così A trasmette i numeri:

$$1^7 \equiv 1, \quad 2^7 \equiv 128, \quad 3^7 \equiv 48, \quad 4^7 \equiv 698 \mod 713$$

B riceve quindi la sequenza di numeri $(1, 128, 48, 698)$ che vuole *decodificare* utilizzando la sua chiave segreta. A questo scopo osserviamo che $ef \equiv 1 \mod \varphi(n) \Leftrightarrow ef = 1 + k\varphi(n)$ e quindi per ogni a

$$(a^f)^e = a^{ef} = a^{1+k\varphi(n)} = a \cdot (a^{\varphi(n)})^k \equiv a \mod n$$

per il teorema di Eulero. Quindi B calcola

$$1^{283} \equiv 1, \quad (128)^{283} \equiv \ldots, \quad (48)^{283} \equiv \ldots, \quad (698)^{283} \equiv (-15)^{283} \ldots \mod 713$$

[19] Sugg. Utilizzare il Teorema 3.12.

[20] Da Rivest Shamir, Adleman i matematici che implementarono il metodo, suggerito da un articolo di Diffie e Hellmann.

[21] in realtà i numeri primi sono molto più grandi, fuori da ogni tabella di numeri primi. Il metodo funziona perchè non si riesce a decomporre un numero nel prodotto di numeri primi in un tempo *ragionevole*.

[22] Si deve calcolare quanti numeri naturali < 713 sono primi con 713. Quindi è ragionevole pensare che, durante la trasmissione, $\varphi(n)$ sia noto solo a B.

Per il calcolo di queste potenze, $\mod n$ scriviamo (come abbiamo già fatto nel test di primalità) $283 = 1 + 2^1 + 2^3 + 2^4 + 2^8$. Quindi $128^{283} = 128 \cdot 128^2 \cdot 128^{2^3} \cdot 128^{2^4} \cdot 128^{2^8} \mod 713$. Si hanno le congruenze mod 713

$$128^1 = 128, \quad 128^2 \equiv -15, \quad 128^{2^2} \equiv 225, \quad 128^{2^3} \equiv 2, \quad 128^{2^4} \equiv 4, \quad 128^{2^5} \equiv 16,$$
$$128^{2^6} \equiv 256, \quad 128^{2^7} \equiv (256)^2 = 2^{16} = 2^{10} \cdot 2^6 \equiv 311 \cdot 2^6 = -182 \cdot 2^4 \equiv -60,$$
$$128^{2^8} \equiv 3600 \equiv 35$$

Quindi:

$$128^{283} \equiv 128 \cdot (-15) \cdot 2 \cdot 4 \cdot 35 = 1024 \cdot (-525) \equiv -311 \cdot 525 = 163275 = 229 \cdot 713 + 2 \equiv 2.$$

Lasciamo al lettore la verifica delle uguaglianze:

$$48^{283} \equiv 3 \mod 713, \quad (-15)^{283} \equiv 4 \mod 713.$$

4 Gruppi abeliani

Sia $(G, +)$ un gruppo abeliano.[23] G si dice finitamente generato se esistono elementi $a_1, \ldots, a_n \in G$ tali che

$$G = \langle \{a_1, \ldots, a_n\} \rangle$$

ossia se e solo se per ogni $g \in G$ esistono $c_1, \ldots, c_n \in \mathbb{Z}$ tali che

$$g = c_1 a_1 + \ldots + c_n a_n.$$

Osserviamo che questa condizione significa che l'applicazione (omomorfismo) ϕ del gruppo $\mathbb{Z}^n = \{(c_1, \ldots, c_n) \mid c_i \in \mathbb{Z}\}$ in G definita da

$$\phi : (c_1, \ldots, c_n) \mapsto c_1 a_1 + \ldots + c_n a_n$$

è un epimorfismo.

Dato che $\langle \{a_1, \ldots, a_n\} \rangle = \langle a_1 \rangle + \ldots + \langle a_n \rangle$ vediamo che ogni gruppo abeliano finitamente generato è somma di gruppi ciclici.

Se G è finitamente generato, un sistema di generatori di G è un insieme $\{a_1, \ldots, a_n\}$ tale che $G = \langle \{a_1, \ldots, a_n\} \rangle$. Degli elementi $a_1, \ldots, a_n \in G$ si dicono linearmente indipendenti se (e solo se) l'omomorfismo ϕ è iniettivo ossia se $c_1 a_1 + \ldots + c_n a_n = 0 \Leftrightarrow c_1 = \ldots = c_n = 0$.

Esempio. Gli elementi (1, 1) e (1, 5) di $\mathbb{Z} \times \mathbb{Z}$ sono linearmente indipendenti perché

$$c_1(1,\, 1) + c_2(1,\, 5) = (c_1 + c_2, c_1 + 5c_2) = (0,\, 0) \Leftrightarrow c_1 = c_2 = 0,$$

ma $\{(1,\, 1), (1,\, 5)\}$ non è un sistema di generatori perché, ad esempio, l'equazione

$$c_1(1,\, 1) + c_2(1,\, 5) = (4,\, 1)$$

non ha soluzioni $(c_1,\, c_2) \in \mathbb{Z} \times \mathbb{Z}$.

[23] È tradizione indicare con + l'operazione in un gruppo abeliano. In particolare si parla di *somma* $a + b$ invece che di prodotto ab di elementi di G, di opposto $-a$ anziché di inverso a^{-1}, di multiplo na anziché di potenza a^n. In particolare l'operazione nella somma $G_1 + \ldots + G_n$ di sottogruppi di G sarà $(g_1, \ldots, g_n) + (\hat{g}_1, \ldots, \hat{g}_n) = (g_1 + \hat{g}_1, \ldots, g_n + \hat{g}_n)$. L'elemento neutro di un gruppo additivo si indica tradizionalmente con 0.

Esercizio. Dimostrare che presi comunque tre elementi di $\mathbb{Z}\times\mathbb{Z}$ questi sono linearmente dpendenti.[24]

Un sistema di generatori $\{a_1,\dots,a_n\}$ si dice *base* di G se l'omomorfismo

$$\phi:\mathbb{Z}^n\to G,\quad \phi(c_1,\dots,c_n)=c_1a_1+\ldots+c_na_n$$

è un isomorfismo. In tal caso si dice che G è un *gruppo libero*. In pratica un gruppo G è libero se e solo se è isomorfo a $\mathbb{Z}^n$ per qualche n. Infatti, posto $e_i=(0,\dots,0,\,1,\,0\dots,0)$ (con 1 nell'i-esima posizione), è facile dimostrare che un omomorfismo $f:\mathbb{Z}^n\to G$ soddisfa

$$f(c_1,\dots,c_n)=f\left(\sum_{i=1}^n c_ie_i\right)=\sum_{i=1}^n c_if(e_i)=\sum_{i=1}^n c_ia_i,\quad a_i:=f(e_i).$$

e quindi è della forma ϕ.

Esempi. i) Abbiamo già visto che gli elementi (1, 1) e (1, 5) di $\mathbb{Z}\times\mathbb{Z}$ sono linearmente indipendenti. Tuttavia l'insieme $\{(1,\,1),(1,\,5)\}$ non è una base di $\mathbb{Z}^2=\mathbb{Z}\times\mathbb{Z}$ in quanto (1, 1) e (1, 5) non generano tutto $\mathbb{Z}^2$. Ma (1, 0) e (0, 1) generano tutto $\mathbb{Z}^2$ e sono linearmente indipendenti. Quindi *non è detto che un insieme di vettori linearmente indipendenti che ha la stessa cardinalità di una base, sia una base.* Tuttavia è vero che due basi di un gruppo libero hanno la stessa cardinalità.

ii) Il gruppo $\mathbb{Z}_6$ è finitamente generato, per esempio $\mathbb{Z}_6=\langle 2,3\rangle$, ma l'insieme $\{2,3\}$ non è una base essendo $3\cdot 2-2\cdot 3=0$. Si osservi che $\mathbb{Z}_6=\langle 1\rangle$ è ciclico.

Osservazione 4.1. . *Dire che G è un gruppo libero significa che ha un insieme di generatori finito $\{a_1,\dots,a_n\}$ e che ogni elemento $a\in G$ si scrive in modo unico come combinazione lineare di $a_1,\dots,a_n$, ossia*

$$G=<a_1>\oplus\ldots\oplus<a_n>\simeq\mathbb{Z}^n.$$

Pertanto G è un gruppo libero se e solo se è somma diretta[25] *di gruppi ciclici infiniti.*

Abbiamo già visto che ogni gruppo abeliano finitamente generato è somma di gruppi ciclici. Si può dimostrare che

Teorema 4.2. *Ogni gruppo abeliano finitamente generato è prodotto di gruppi ciclici (anche nel caso in cui il gruppo non sia libero).*

Per esempio consideriamo un gruppo (supponiamo moltiplicativo[26]) G di *ordine pari*. G ha $2n$ elementi di cui $2n-1$ diversi dall'unità. Ad ogni elemento $x\in G$, $x\neq e$ associamo l'insieme $I_x:=\{x,x^{-1}\}$. Ovviamente, se $x,x^{-1}\neq y$ si ha $I_x\cap I_y=\emptyset$. Sia $S\subset G$ tale che[27] $G-\{e\}=\dot{\bigcup}_{x\in S}I_x$. Se tutti gli insiemi I_x, $x\in S$, avessero cardinalità 2 si avrebbe

$$2n-1=|G-\{e\}|=\left|\dot{\bigcup}_{x\in S}I_x\right|=2|S|$$

[24]Siano $(a_1,\,b_1)$, $(a_2,\,b_2)$, $(a_3,\,b_3)$ gli elementi di $\mathbb{Z}\times\mathbb{Z}$. Si tratta di dimostrare che esistono $c_1,c_2,c_3\in\mathbb{Z}$ soluzioni del sistema

$$\begin{cases} c_1a_1+c_2a_2+c_3a_3=0\\ c_1b_1+c_2b_2+c_3b_3=0.\end{cases}$$

Si provi che il sistema ammette una soluzione $(\bar c_1,\,\bar c_2,\,\bar c_3)\in\mathbb{Q}^3$. Quindi, indicando con d il minimo comune multiplo dei denominatori di $\bar c_1,\bar c_2,\bar c_3$ una soluzione intera del sistema è ...

[25]o prodotto

[26]Scrivere lo stesso ragionamento quando G è un gruppo additivo

[27]Il simbolo $\dot{\bigcup}$ significa *unione disgiunta* ossia $X=\dot{\bigcup}_{\alpha\in A}T_\alpha$ significa che $X=\bigcup_{\alpha\in A}T_\alpha$ e $\alpha\neq\alpha'\Rightarrow T_\alpha\cap T_{\alpha'}=\emptyset$.

che è assurdo. Quindi deve esistere $x \in G$ tale che $x = x^{-1}$. Se H è un altro sottogruppo di G tale che $x \notin H$ si ha $H + < x >= H \oplus < x >= H \oplus \{1, x\}$. Si ha quindi $|H \oplus < x >| = 2|H|$. Provare che la funzione

$$H \times < x > \to G, \quad (h, t) \mapsto ht$$

è un omomorfismo iniettivo. Quindi se $|H| = n$ si ha $G \simeq H \times < x >$. In particolare se H è prodotto di gruppi ciclici anche G lo è. Come esempio consideriamo il gruppo $\mathbb{Z}_{32}^*$. Si ha $15^2 = 225 \equiv 1 \mod 32$. Ricerchiamo un sottogruppo ciclico di $\mathbb{Z}_{32}^*$ di ordine 8 che non contenga 15. Per esempio:

$$< 3 >= \{1, 3, 9, 11, 17, 19, 25, 27\}$$

Verificare che

$$< 3 > \times < 15 > \to \mathbb{Z}_{32}^*, (3^h, t) \mapsto 3^h t$$

con $h = 1, \ldots, 8$ e $t = 1, 15$ è un isomorfismo.

Esempi. i) Provare che $\mathbb{Z}_{64}^* \simeq < 3 > \times < 31 >$. Si noti che l'operazione in $< 3 > \times < 31 >$ è $(3^i, 31^j) \odot (3^h, 31^k) = (3^{i+h}, 31^{j+k})$ e l'isomorfismo fra $< 3 > \times < 31 >$ e $\mathbb{Z}_{64}^*$ è $(3^h, 31^k) \mapsto 3^h \cdot 31^k$.[28]

Osservazione 4.3. *Un gruppo abeliano finito G è certamente finitamente generato (un insieme di generatori è certamente G) e quindi è prodotto di gruppi ciclici* finiti. *D'altronde un gruppo ciclico finito è isomorfo a $\mathbb{Z}_m$ (per qualche $m \in \mathbb{Z}$). Pertanto si può scrivere:*

$$G = \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}$$

ma decomponendo m_k nel prodotto di fattori primi e utilizzando il Teorema 3.12-i) otteniamo che

$$G = \Pi_{j=1}^n \mathbb{Z}_{p_j^{h_j}}.$$

dove i p_j sono primi (non necessariamente distinti) e $h_j \in \mathbb{N}$.

Esempio. Abbiamo visto che $\mathbb{Z}_{32}^* \simeq < 3 > \times < 15 >$. Il primo è un gruppo ciclico di ordine 2, il secondo di ordine 8 (un generatore è 3). Quindi:

$$\mathbb{Z}_{32}^* \simeq \mathbb{Z}_8 \times \mathbb{Z}_2 = \mathbb{Z}_{2^3} \times \mathbb{Z}_2.$$

<u>*Esercizio*</u>. Determinare, se possibile, un gruppo abeliano di ordine 60 con esattamente 2 elementi di ordine 2.[29] Quanti elementi ha di ordine 3?

5 Caratteri su gruppi abeliani finiti

Sia $(G, \cdot)$ un gruppo abeliano. Per comodità utilizzeremo la notazione moltiplicativa. Un *carattere* su G è un omomorfismo di gruppi $\chi : G \to \mathbb{C}^*$, di G nel gruppo moltiplicativo dei numeri complessi non nulli.[30]

[28] Si osservi che $< 31 >= \{1, 31\}$ e $31 \notin < 3 >$. Quindi $< 3 > + < 31 > = < 3 > \oplus < 31 > = \{(3^h, 1), (3^k, 31) \mid h, k \in \mathbb{Z}\}$.

[29] Si scriva $60 = 2^2 \cdot 3 \cdot 5$ quindi un gruppo G di ordine 60 è isomorfo a ... oppure a ...

[30] Il motivo per cui si considerano gruppi abeliani è perché altrimenti potrebbero esserci *pochi* caratteri. Infatti supponiamo che G sia un gruppo semplice (ossia senza sottogruppi non banali) non commutativo. Un omomorfismo $\chi : G \to \mathbb{C}^*$ avrà un nucleo che, per la semplicità di G, dovrà essere $\ker \chi = \{e\}$ oppure $\ker \chi = G$. Supponiamo che $\ker \chi = \{e\}$ e siano $g, h \in G$. Dato che $\chi(g^{-1}hgh^{-1}) = \chi(g^{-1})\chi(h)\chi(g)\chi(h)^{-1} = 1$ si ottiene $g^{-1}hgh^{-1} = e$ ossia $hg = gh$ contrariamente all'ipotesi di non abelianità. Allora $\ker \chi = G$. Ossia l'unico carattere è l'applicazione $\chi(g) = 1$ per ogni $g \in G$.

Esempio. Sia G un gruppo abeliano finito di ordine n. Sia χ un carattere su G. Per ogni $a \in G$ si ha $a^n = e$ (cfr Corollario 2.2) e quindi:

$$1 = \chi(e) = \chi(a^n) = \chi(a)^n$$

quindi $\chi(a)$ è una radice $n-$esima dell'unità: $\chi(a) = \mathrm{e}^{\frac{2k\pi i}{n}}$, per qualche $k \in \{0, \dots, n-1\}$. In particolare $\chi : G \to S^1$, il sottogruppo (moltiplicativo) di $\mathbb{C}^*$ dei numeri complessi di modulo 1.

Nell'insieme dei caratteri su G possiamo definire un'operazione *elemento per elemento* come si fa con le funzioni. Se χ_1 e χ_2 sono due caratteri su G il simbolo $\chi_1\chi_2$ indica il carattere

$$\chi_1\chi_2 : g \mapsto \chi^1(g)\chi_2(g) \in \mathbb{C}^*.$$

Con questa operazione l'insieme dei caratteri su G diventa un gruppo. L'elemento neutro è l'omomorfismo costante: $\varepsilon(g) = 1$ per ogni $g \in G$. ε si dice *carattere principale.* L'inverso di $\chi : G \to \mathbb{C}^*$ è l'omomorfismo:

$$\chi^{-1} : g \mapsto \chi(g)^{-1} = \overline{\chi(g)} \tag{9}$$

(dato che $|\chi(g)| = 1$). Il gruppo dei caratteri su G si indica con $\widehat{G}$ ed è un gruppo abeliano dato che la moltiplicazione in $\mathbb{C}^*$ è commutativa. Sia $H < G$ un sottogruppo di G. La restrizione ad H di un carattere su G definisce un carattere su H. Quindi resta definita un'applicazione:

$$\widehat{G} \to \widehat{H}, \chi \mapsto \chi_{|H}.$$

Si ha il seguente

Teorema 5.1. *Sia $H < G$ e supponiamo che $[G : H]$ sia finito. Ogni carattere su H si può estendere ad un carattere su G in $[G : H]$ modi diversi.*

Dimostrazione (del Teorema 5.1). Procediamo per induzione su $[G : H]$. Se $[G : H] = 1$ si ha $H = G$ e non è nulla da dimostrare. Quindi supponiamo $H \neq G$. Scegliamo $a \in G \setminus H$ cosicchè

$$H < H + \langle a \rangle < G.$$

Sia $\chi : H \to \mathbb{C}^*$ un carattere su H. Ci proponiamo di estendere χ a $\tilde{\chi} : H + < a > \to C^*$ e di contare i modi diversi di farlo. Dato che $[G : H]$ è finito le classi laterali $H, aH, a^2H, \dots a^kH, \dots$ non sono tutte distinte e quindi esiste $k \in \mathbb{N}$, $k \geq 2$, (ad esempio $k = [G : H]$) tale che $a^k \in H$. Scegliamo il valore di k più piccolo tale che $a^k \in H$ (in pratica $k = [H + \langle a \rangle : H]$). Quindi una qualunque estensione $\tilde{\chi}$ di χ deve soddisfare $\tilde{\chi}(a)^k = \tilde{\chi}(a^k) = \chi(a^k)$. Poniamo allora $\tilde{\chi}(a) = z$ con $z^k = \chi(a^k)$. Ovviamente abbiamo k soluzioni diverse dell'equazione (in C^*) $z^k = \chi(a^k)$ e ciò significa che abbiamo k possibili scelte (differenti) per $\tilde{\chi}(a)$. Sia ζ una di queste scelte e poniamo

$$\tilde{\chi}(ha^i) = \chi(h)\zeta^i \in C^*. \tag{10}$$

Chiaramente $\tilde{\chi}_{|H} = \chi$, ma occorre provare che questa è una buona definizione di $\tilde{\chi}$. Questo è necessario perché potrebbe succedere che $H \cap < a > \neq \{e\}$ (se $a^k \neq e$). Ora, se per $0 < i < j$ si avesse

$$h_1a^i = h_2a^j$$

risulterebbe $H \ni h_2^{-1}h_1 = a^{j-i}$ da cui $k \mid j - i \mod k$ e $h_1 = h_2a^{j-i}$. Scriviamo $j - i = kq$. Si ha:

$$\tilde{\chi}(h_1a^i) = \chi(h_1)\zeta^i = \chi(h_2a^{j-i})\zeta^i = \chi(h_2a^{kq})\zeta^i = \chi(h_2)\chi(a^k)^q\zeta^i = \chi(h_2)(\zeta^k)^q\zeta^i = \chi(h_2)\zeta^{kq+i} = \chi(h_2)\zeta^j.$$

Pertanto la (10) è una buona definizione di $\tilde{\chi}$. Occorre mostrare che definisce un omomorfismo di $H + < a >$ in C^*. Se h_1a^i e h_2a^j sono elementi di $H + < a >$, con $0 \leq i, j < k$, si ha

$$(h_1a^i) \cdot (h_2a^j) = h_1h_2a^{\delta k}a^\ell$$

dove $\ell = i + j \mod k$ e $\delta = 0, 1$. Ma allora

$$\tilde{\chi}(h_1 a^i)\tilde{\chi}(h_2 a^j) = \chi(h_1)\chi(h_2)\zeta^i\zeta^j = \chi(h_1 h_2)\zeta^{\delta k}\zeta^\ell = \chi(h_1 h_2 a^{\delta k})\zeta^\ell = \tilde{\chi}(h_1 h_2 a^{\ell+\delta k}) = \tilde{\chi}(h_1 a^i \cdot h_2 a^j).$$

Abbiamo provato che esistono (esattamente) $[H+ < a >: H]$ estensioni differenti di χ a $H+ < a >$. Dato che $[G : H+ < a >] < [G : H]$, per l'ipotesi di induzione esistono (esattamente) $[G : H+ < a >]$ modi differenti di estendere $\tilde{\chi}$ da $H+ < a >$ a G. In totale $\chi : H \to \mathbb{C}^*$ si può estendere in (esattamente) $[G : H+ < a >][H+ < a >: H] = [G : H]$ modi ad un carattere su G. □

Corollario 5.2. *Sia G un gruppo abeliano finito. Se $e \neq g \in G$ esiste un carattere χ su G tale che $\chi(g) \neq 1$. Il numero dei caratteri di G è $|G|$.*

Dimostrazione. Dato che G è finito esiste $n \mid |G|$ tale che $g^n = e$ (e $g^k \neq e$ per ogni $k = 1, \ldots, n-1$). Definiamo un carattere su G ponendo $\chi(g) = \zeta$, $\zeta^n = 1$, $\zeta \neq 1$ (ci sono $n-1$ tali scelte). Per il Teorema 5.1 possiamo estendere χ ad un carattere su G che chiaramente soddisfa $\chi(g) \neq 1$. La seconda parte segue sempre dal Teorema 5.1 scegliendo $H = \{e\}$ (e $\chi(e) = 1$). □

Corollario 5.3. *Sia G un gruppo abeliano finito, $H < G$ e $g \in G$ tale che $g \notin H$. Allora esiste un carattere χ su G tale che $\chi(g) \neq 1$ e $\chi_{|H} = 1$*

Dimostrazione. Consideriamo i gruppi H e $H + \langle g \rangle$. Dato che $g \notin H$ si ha $[H + \langle g \rangle : H] > 1$. Dal Teorema 5.1 il carattere principale su H, $\chi(h) = 1$ per ogni $h \in H$, si estende in $[H + \langle g \rangle : H] > 1$ modi ad un carattere su $H + \langle g \rangle$. Scegliamo uno di questi modi in modo che $\chi(g) \neq 1$. Applicando ancora il Teorema 5.1 un tale carattere si estende ad uno su G che, ovviamente, soddisfa: $\chi(h) = 1$ e $\chi(g) \neq 1$. □

Corollario 5.4. *Sia G un gruppo abeliano finito e $g \in G$ tale che $g \neq g_2$ due elementi di G. Allora esiste un carattere χ su G tale che $\chi(g_1) \neq \chi(g_2)$*

Dimostrazione. Si applichi il Corollario 5.2 a $g = g_1 g_2^{-1}$. □

Teorema 5.5. *Siano G_1 e G_2 due gruppi abeliani. La funzione $\Phi : \widehat{G}_1 \times \widehat{G}_2 \to \widehat{G_1 \times G_2}$ definita da:*

$$\Phi : (\chi_1, \chi_2) \mapsto (\chi_1\chi_2)(g_1, g_2) := \chi_1(g_1)\chi_2(g_2) \in \mathbb{C}^*.$$

è un isomorfismo

Dimostrazione. È facile verificare che $\Phi(\chi_1, \chi_2)$ è un omomorfismo. Se $\Phi(\chi_1, \chi_2)(g_1, g_2) = 1$ per ogni $(g_1, g_2) \in G_1 \times G_2$ s avrà anche

$$\chi_1(g_1) = \chi_1(g_1)\chi_2(e_2) = \Phi(\chi_1, \chi_2)(g_1, e_2) = 1$$

per ogni $g_1 \in G_1$ e similmente $\chi_2(g_2) = 1$ per ogni $g_2 \in G_2$. Quindi $\ker \Phi = \{(\varepsilon_1, \varepsilon_2)\}$. Se $\chi : G_1 \times G_2 \to \mathbb{C}^*$ è un omomorfismo, definiamo $\chi_1 : G_1 \to \mathbb{C}^*$ e $\chi_2 : G_2 \to \mathbb{C}^*$ come segue:

$$\chi_1(g_1) = \chi(g_1, e_2), \qquad \chi_2(g_2) = \chi(e_1, g_2).$$

Si ha $\chi_1 \in \widehat{G}_1$ e $\chi_2 \in \widehat{G}_2$ e

$$(\chi_1\chi_2)(g_1, g_2) = (\chi_1\chi_2)[(g_1, e_2) \cdot (e_1, g_2)] = (\chi_1\chi_2)(g_1, e_2)(\chi_1\chi_2)(e_1, g_2) = \chi_1(g_1)\chi_2(g_2) = \chi(g_1, g_2).$$

per cui Φ è suriettiva. □

Nel paragrafo precedente abbiamo visto che ogni gruppo abeliano è prodotto di gruppi ciclici: $G = \langle a_1 \rangle \times \ldots \times \langle a_n \rangle$. Si ha allora

$$\widehat{G} = \widehat{\langle a_1 \rangle} \times \ldots \times \widehat{\langle a_n \rangle}.$$

Lemma 5.6. *Sia $G = \langle a \rangle$ un gruppo abeliano ciclico finito. Allora $\widehat{G} \simeq G$.*

Dimostrazione. Sia n l'ordine di a cosicché $G = \{e, a, \ldots, a^{n-1}\}$. Sia $\theta = \mathrm{e}^{\frac{2\pi i}{n}}$ e $\chi_a : G \to S^1$, $\chi_a(a^k) = \theta^k$. Dato che $\theta^n = 1$ è chiaro che χ_a è un carattere su G. Se χ è un qualsiasi carattere su G si avrà $\chi(a)^n = 1$ e quindi esiste $h \in \{0, 1, \ldots, n-1\}$ tale che $\chi(a) = \mathrm{e}^{\frac{2h\pi i}{n}}$. Ma allora, per ogni j

$$\chi(a^j) = \chi(a)^j = \mathrm{e}^{\frac{2hj\pi i}{n}} = \chi_a(a^j)^h = \chi_a^h(a^j)$$

ossia $\chi = \chi_a^j$. In particolare $\widehat{G} = \langle \chi_a \rangle$. L'applicazione $G \to \widehat{G}$, $a^k \mapsto \chi_a^k$ è un isomorfismo di gruppi. Infatti, per quanto abbiamo visto è suriettiva e:

$a^{i+j} \mapsto \chi_a^{i+j} = \chi_a^i \chi_a^j$;

Se $\chi_a^k(a^i) = 1$ per ogni $i = 0, \ldots, n-1$ risulta $\theta^{ki} = 1$ per ogni $i = 0, \ldots, n-1$. Pertanto $k \equiv 0 \mod n$ ossia $a^k \mapsto \chi_a^k$ è iniettiva.

Corollario 5.7. *Sia G un gruppo abeliano finito. Allora $\widehat{G} \simeq G$.*

Dimostrazione. Sappiamo che $G = \langle a_1 \rangle \times \ldots \times \langle a_n \rangle$ e quindi $\widehat{G} = \widehat{\langle a_1 \rangle} \times \ldots \times \widehat{\langle a_n \rangle}$. La conclusione segue dal fatto che ogni $\langle a_i \rangle$ è isomorfo a $\widehat{\langle a_i \rangle}$. □

Esempio. Determinare $\widehat{G}$ con $G = \mathbb{Z}_8^*$. Si ha $\mathbb{Z}_8^* \simeq \mathbb{Z}_3^* \times \mathbb{Z}_3^*$ e $\mathbb{Z}_3^* = \{\varepsilon, \chi\}$, dove:

$$\chi(1) = 1, \quad \chi(2) = -1.$$

Allora $\widehat{\mathbb{Z}_8^*} = \{(\varepsilon, \varepsilon), (\varepsilon, \chi), (\chi, \varepsilon), (\chi, \chi)\}$. È conveniente illustrare i quattro caratteri con una tabella che contenga solo gli elementi di $\mathbb{Z}_8^*$:

	1	3	5	7
ε	1	1	1	1
χ_1	1	1	-1	-1
χ_2	1	-1	1	-1
χ_3	1	-1	-1	1

Tabella 1: Tabella dei caratteri di $\mathbb{Z}_8^*$.

Allo stesso risultato si arriva considerando che: $\mathbb{Z}_8^* = \langle 3 \rangle \times \langle 5 \rangle = \{1, 3\} \times \{1, 5\}$ (si noti che $3 \cdot 5 \equiv 7 \mod 8$). Un insieme di generatori di $\mathbb{Z}_8^*$ è $\{3, 5\}$ entrambi di periodo 2 quindi un qualsiasi carattere χ su $\mathbb{Z}_8^*$ deve soddisfare $\chi(3) = 1$ o $\chi(3) = -1$ e $\chi(5) = 1$ o $\chi(5) = -1$. Noti questi due valori si ottiene $\chi(7)$ da $\chi(7) = \chi(3 \cdot 5) = \chi(3) \cdot \chi(5)$. Verificare che si ottiene la stabella precedente.

Similmente determiniamo i caratteri di $\mathbb{Z}_{16}^* = \langle 3 \rangle \times \langle 7 \rangle$. Osserviamo che

$$\langle 3 \rangle = \{1, 3, 9, 11\} \quad \text{e} \quad \langle 7 \rangle = \{1, 7\}.$$

Quindi un qualsiasi carattere su $\mathbb{Z}_{16}^*$ assume su 3 uno fra i valori $\{\pm 1, \pm i\}$ mentre su 7 uno fra i valori dell'insieme $\{\pm 1\}$. Quindi, osservando che

$$9 \equiv 3^2, \quad 11 \equiv 3^3, \quad 5 \equiv 3 \cdot 7, \quad 13 \equiv 7 \cdot 11, \quad 15 \equiv 7 \cdot 9 \quad \mod 16$$

otteniamo la Tabella 2.

Esercizio. Costruire la tabella dei caratteri del gruppo $\mathbb{Z}_8^* \times \mathbb{Z}_8^*$ e quella del gruppo $\mathbb{Z}_3^* \times \mathbb{Z}_3^* \times \mathbb{Z}_3^*$.

L'isomorfismo $G \to \widehat{G}$ di un gruppo abeliano finito nel suo gruppo dei caratteri $\widehat{G}$ non è *canonico* in quanto dipende dalla scelta dei generatori dei gruppi ciclici il cui prodotto è G (un po' come gli isomorfismi tra uno spazio vettoriale V e il suo duale V^* dipendono dalla scelta della base di V). Ora assegnato un gruppo abeliano finito G e indicato con $\widehat{G}$ il suo gruppo dei caratteri, anche $\hat{G}$ è abeliano e quindi possiamo costruire il gruppo dei caratteri $\widehat{\widehat{G}}$. Si ha il seguente

	1	3	5	7	9	11	13	15
ε	1	1	1	1	1	1	1	1
χ_1	1	-1	-1	1	1	-1	-1	1
χ_2	1	i	i	1	-1	-i	-i	-1
χ_3	1	-i	-i	1	-1	i	i	-1
χ_4	1	1	-1	-1	1	1	-1	-1
χ_5	1	-1	1	-1	1	-1	1	-1
χ_6	1	i	-i	-1	-1	-i	i	1
χ_7	1	-i	i	-1	-1	i	-i	1

Tabella 2: Tabella dei caratteri di $\mathbb{Z}_{16}^*$.

Teorema 5.8. *Sia G un gruppo abeliano finito. L'applicazione $G \to \widehat{\widehat{G}}$ definita da $g \mapsto \hat{g}$ dove $\hat{g} : \widehat{G} \to \mathbb{C}^*$ è definita da $\hat{g}(\chi) = \chi(g)$ è un isomorfismo di gruppi abeliani.*

Dimostrazione. Si ha $\widehat{g_1 g_2}(\chi) = \chi(g_1 g_2) = \chi(g_1)\chi(g_2) = \widehat{g}_1(\chi)\widehat{g}_2(\chi)$ per ogni $\chi \in \widehat{G}$. Quindi $\widehat{g_1 g_2} = \widehat{g}_1 \widehat{g}_2$ ossia $g \mapsto \hat{g}$ è un omomorfismo di gruppi. Se $\hat{g}(\chi) = 1$ per ogni $\chi \in \widehat{G}$ significa che $\chi(g) = 1$ per ogni $\chi \in \hat{G}$ e quindi per il Corollario 5.3, $g = e$. L'omomorfismo $g \mapsto \hat{g}$ è quindi iniettivo e dato che $|\widehat{\widehat{G}}| = |\widehat{G}| = |G|$ è anche suriettivo e perciò un isomorfismo. □

Osserviamo che l'isomorfismo del Teorema 5.8 non dipende dalla scelta di un sistema di generatori di $\widehat{G}$: è un *isomorfismo canonico* (anche in questo caso analogamente agli spazi vettoriali).

Teorema 5.9. *Sia G un gruppo abeliano finito. Allora per ogni carattere $\chi \in \widehat{G}$ si ha*

$$\frac{1}{|G|}\sum_{g\in G}\chi(g) = \begin{cases} 1 & \text{se } \chi = \varepsilon \\ 0 & \text{se } \chi \neq \varepsilon \end{cases}$$

e per ogni $g \in G$ si ha

$$\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\chi(g) = \begin{cases} 1 & \text{se } g = e \\ 0 & \text{se } g \neq e. \end{cases}$$

Dimostrazione. Si ha $\varepsilon(g) = 1$ per ogni $g \in G$ e quindi

$$\sum_{g\in G}\varepsilon(g) = |G|.$$

Se invece $\chi \neq \varepsilon$ esiste $h \in G$ tale che $\chi(h) \neq 1$. Dato che la funzione $g \mapsto hg$ è una biiezione di G in G si ha

$$\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(hg) = \chi(h)\sum_{g\in G}\chi(g)$$

e questo implica che $\sum_{g\in G}\chi(g) = 0$ perchè $\chi(h) \neq 1$. La seconda parte segue dalla prima tenendo conto dell'uguaglianza:

$$\frac{1}{|G|}\sum_{g\in G}\chi(g) = \frac{1}{|\widehat{\widehat{G}}|}\sum_{\hat{g}\in\widehat{\widehat{G}}}\hat{g}(\chi).$$

e $\hat{g}(\chi) = 1\ \forall \chi \in \widehat{G} \ \Leftrightarrow\ g = e$. □

Il Teorema 5.9 afferma essenzialmente che la somma degli elementi di riga (o di colonna) nella tabella dei caratteri è zero tranne che per la riga di ε (o la colonna di e). Si verifichi questa proprietà dei caratteri nelle tabelle che abbiamo costruito.

Il Teorema 5.9 si estende facilmente (stessa dimostrazione) ai sottogruppi:

Teorema 5.10. *Siano G un gruppo abeliano finito, $H < G$ e $K < \widehat{G}$ sottogruppi di G e $\widehat{G}$ rispettivamente. Allora per ogni carattere $\chi \in \widehat{G}$ si ha*

$$\frac{1}{|H|}\sum_{h\in H}\chi(h) = \begin{cases} 1 & \text{se } \chi_H = \varepsilon \\ 0 & \text{se } \chi_H \neq \varepsilon \end{cases}$$

e per ogni $g \in G$ si ha

$$\frac{1}{|K|}\sum_{\chi\in K}\chi(g) = \begin{cases} 1 & \text{se } \chi(g) = 1 \text{ per ogni } \chi \in K \\ 0 & \text{altrimenti.} \end{cases}$$

Per esempio, riferendosi alla tabella dei caratteri su $\mathbb{Z}_{16}^*$ $\varepsilon, \chi_1, \chi_2, \chi_3$ sono identicamente uguali ad 1 su $H = \{1, 7\}$, mentre $\chi_4, \chi_5, \chi_6, \chi_7$ non lo sono. Si ha $\chi(1)+\chi(7) = 2 = |H|$ per le prime 4 righe mentre $\chi(1) + \chi(7) = 0$ per le ultime 4. Scegliendo $K = \{\varepsilon, \chi_4\}$ o $K = \{\varepsilon, \chi_5\}$ si verifichi che la somma, per colonna, degli elementi che stanno nelle righe corrispondenti agli elementi di K soddisfa la conclusione del Teorema 5.10. Per la dimostrazione del Teorema 5.10 basta osservare che, in virtù dell'isomorfismo $G \simeq \widehat{\widehat{G}}$ ogni sottogruppo $K < \widehat{G}$ è del tipo $\widehat{\widehat{H}}$, con $H < G$.

<u>*Esercizio*</u>. Siano G un gruppo abeliano finito e $g \in G$. Provare che $g^k = 1$ se e solo se $\chi^k(g) = 1$ per ogni $\chi \in \widehat{G}$. Per dualità dimostrare quindi che $\chi^k = \varepsilon$ se e solo se $\chi(g^k) = 1$ per ogni $g \in G$.

Le proprietà dei caratteri di un gruppo abeliano permettono di costruire una teoria analoga a quella delle trasformate di Fourier delle funzioni periodiche. Una funzione periodica può essere vista come una funzione di S^1 in $\mathbb{C}$ ed S^1 è un gruppo abeliano (non finitamente generato avendo la cardinalità del continuo $S^1 = \{e^{i\theta} \mid 0 \leq \theta < 2\pi\}$). Quindi quello che segue può essere visto, da una parte come una particolarizzazione delle trasformate di Fourier a gruppi finiti, dall'altra come un'estensione a gruppi abeliani prodotto diretto di gruppi ciclici.

Siano $f, f_1, f_2 : G \to \mathbb{C}$ funzioni di un gruppo G nel campo dei numeri complessi. Definiamo

$$\langle f_1, f_2\rangle = \sum_{g\in G} f_1(g)\overline{f_2(g)}$$

e:[31]

$$\hat{f} : \widehat{G} \to \mathbb{C}, \quad \hat{f}(\chi) := \langle f, \chi\rangle = \sum_{g\in G} f(g)\overline{\chi(g)} = \sum_{g\in G} f(g)\chi(g^{-1})$$

(cfr. eq. (9)). Si osservi che

$$\begin{aligned}\langle \lambda f_1 + \mu f_2, f_3\rangle &= \lambda\langle f_1, f_3\rangle + \mu\langle f_2, f_3\rangle \\ \langle f_1, \lambda f_2 + \mu f_3\rangle &= \bar{\lambda}\langle f_1, f_2\rangle + \bar{\mu}\langle f_2, f_3\rangle\end{aligned}$$

ossia il prodotto scalare $\langle\cdot,\cdot\rangle$ è lineare nella prima componente e coniugato-lineare nella seconda.

Per comodità indichiamo con $\bar{\chi} = \chi^{-1}$ il carattere definito da

$$\bar{\chi}(g) := \overline{\chi(g)} = \chi^{-1}(g) = \chi(g^{-1}).$$

cosicché:

$$\hat{f}(\chi) := \langle f, \chi\rangle = \sum_{g\in G} f(g)\bar{\chi}(g). \tag{11}$$

[31] si noti l'analogia con le definizioni

$$\begin{aligned}\langle f, g\rangle &= \int_{-\infty}^{\infty} f(t)\overline{g(t)}dt \\ \hat{f}(\omega) &= \int_{-\infty}^{\infty} f(t)e^{-i\omega t}dt.\end{aligned}$$

La funzione $\hat{f} : \widehat{G} \to \mathbb{C}$ definita da $\hat{f}(\chi) = \langle f, \chi \rangle$ si dice *trasformata di Fourier di* f.

Siano $g_1, g_2 \in G$ due elementi di un gruppo abeliano finito G e χ_1, χ_2 due caratteri su G. Dato che

$$
\begin{aligned}
\langle \chi_1, \chi_2 \rangle &= \sum_{g \in G} \chi_1(g)\overline{\chi_2(g)} = \sum_{g \in G} [\chi_1 \chi_2^{-1}](g) \\
\langle \widehat{\widehat{g_1}}, \widehat{\widehat{g_2}} \rangle &= \sum_{\chi \in \widehat{G}} \widehat{\widehat{g_1}}(\chi)\overline{\widehat{\widehat{g_2}}(\chi)} = \sum_{\chi \in \widehat{G}} \chi(g_1)\overline{\chi(g_2)}
\end{aligned} \tag{12}
$$

dal Teorema 5.9 otteniamo subito il seguente:

Teorema 5.11. *Siano $g_1, g_2 \in G$ due elementi di un gruppo abeliano finito G e χ_1, χ_2 due caratteri su G. Allora:*

$$
\begin{aligned}
\frac{1}{|G|} \sum_{g \in G} \chi_1(g)\overline{\chi_2(g)} &= \begin{cases} 1 & \text{se } \chi_1 = \chi_2 \\ 0 & \text{se } \chi_1 \neq \chi_2 \end{cases} \\
\frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(g_1)\overline{\chi(g_2)} &= \begin{cases} 1 & \text{se } g_1 = g_2 \\ 0 & \text{se } g_1 \neq g_2 \end{cases}
\end{aligned}
$$

Dimostrazione. Lasciata al lettore. Si basa sulle (12). □

Esempio. Siano $a, b \in \mathbb{Z}_m^*$ (ossia $\gcd(a, m) = 1$, $\gcd(b, m) = 1$). Allora:

$$
\frac{1}{\varphi(m)} \sum_{\chi \in \widehat{\mathbb{Z}_m^*}} \chi(a)\bar{\chi}(b) = \begin{cases} 1 & \text{se } a = b \\ 0 & \text{se } a \neq b \end{cases}
$$

In particolare la formula precedente vale se p è un numero primo che non divide m. L'uguaglianza

$$
\frac{1}{\varphi(m)} \sum_{\chi \in \widehat{\mathbb{Z}_m^*}} \chi(p)\bar{\chi}(a) = \begin{cases} 1 & \text{se } a = p \\ 0 & \text{se } a \neq p \end{cases}
$$

è stata utilizzata da Dedekind nella dimostrazione dell'esistenza di infiniti primi nella successione $a + bn$ con $\gcd(a, b) = 1$.

Dal Teorema 5.11 otteniamo

$$
\begin{aligned}
f(x) &= \frac{1}{|G|} \sum_{g \in G} f(g) \sum_{\chi \in \hat{G}} \chi(x)\bar{\chi}(g) = \frac{1}{|G|} \sum_{g \in G} \sum_{\chi \in \hat{G}} f(g)\bar{\chi}(g)\chi(x) \\
&= \frac{1}{|G|} \sum_{\chi \in \hat{G}} \left[\sum_{g \in G} f(g)\bar{\chi}(g) \right] \chi(x) = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \langle f, \chi \rangle \chi(x) = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi(x).
\end{aligned}
$$

L'uguaglianza[32]

$$
f(x) = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi(x). \tag{13}
$$

si dice *formula d'inversione di Fourier* (la (11) è la formula della trasformata di Fourier).

La formula di inversione (13) non è l'unica analogia con la teoria di Fourier classica. Infatti si ha:

[32] si noti l'analogia con la formula di inversione delle TdF:

$$
f(t) = \frac{1}{2\pi} v.p. \int_{-\infty}^{\infty} \hat{f}(\omega) e^{i\omega t} d\omega.
$$

Teorema 5.12 (Plancherel)**.** *Siano $f_1, f_2 : G \to \mathbb{C}$. Allora*

$$\langle f_1, f_2\rangle = \frac{1}{|G|}\langle \widehat{f_1}, \widehat{f_2}\rangle \tag{14}$$

Dimostrazione. Dalla (13) si ha

$$\langle f_1, f_2\rangle = \frac{1}{|G|^2}\langle \sum_{\chi\in\hat{G}} \hat{f}_1(\chi)\chi, \sum_{\chi\in\hat{G}} \hat{f}_2(\chi)\chi\rangle = \frac{1}{|G|^2}\sum_{\chi,\psi\in\hat{G}} \hat{f}_1(\chi)\overline{\hat{f}_2(\psi)}\langle\chi,\psi\rangle$$

ma dal Teorema 5.11

$$\langle \chi, \psi\rangle = \sum_{g\in G}\chi(g)\overline{\psi(g)} = \begin{cases} |G| & \text{se } \chi = \psi \\ 0 & \text{se } \chi \neq \psi \end{cases}$$

pertanto

$$\langle f_1, f_2\rangle = \frac{1}{|G|}\sum_{\chi,\psi\in\hat{G}} \hat{f}_1(\chi)\overline{\hat{f}_2(\psi)} = \frac{1}{|G|}\langle \widehat{f_1}, \widehat{f_2}\rangle. \quad \square$$

E quindi con $f_1 = f_2$:

Teorema 5.13 (Parseval)**.** *Sia $f : G \to \mathbb{C}$. Allora*

$$\sum_{g\in G}|f(g)|^2 = \frac{1}{|G|}\sum_{\chi\in\hat{G}}|\hat{f}(\chi)|^2. \tag{15}$$

Esempio. Consideriamo il gruppo $G = (\mathbb{Z}_m, +)$ Un carattere è un omomorfismo di $\mathbb{Z}_m \to \mathbb{C}^*$. Per il Corollario 5.7 si ha $\widehat{\mathbb{Z}}_m \simeq \mathbb{Z}_m$ ed anzi, essendo $\mathbb{Z}_m = \langle 1\rangle$ si ha $\widehat{\mathbb{Z}}_m = \langle\chi\rangle$ dove $\chi(1) = \mathrm{e}^{\frac{2\pi i}{m}}$ e $\chi(j) = \chi(1)^j = \mathrm{e}^{\frac{2\pi i j}{m}}$. Quindi $\widehat{\mathbb{Z}}_m = \{\varepsilon = \chi^0, \chi, \ldots, \chi^{m-1}\}$. L'isomorfismo $j \in \chi^j$ di $\mathbb{Z}_m$ in $\widehat{\mathbb{Z}}_m$ permette di identificare χ^j con j e quindi di vedere $\hat{f} : \mathbb{Z}_m \to \mathbb{C}$ invece che $\hat{f} : \widehat{\mathbb{Z}}_m \to \mathbb{C}$[33] Ad esempio si consideri $f : \mathbb{Z}_4 \to \mathbb{C}$ definita come nella tabella seguente:

	0	1	2	3
f	i	-1	i	-1

La tabella dei caratteri di $\mathbb{Z}_4$ è

	0	1	2	3
ε	1	1	1	1
χ	1	$\mathrm{e}^{\frac{\pi i}{2}}$	$\mathrm{e}^{\pi i}$	$\mathrm{e}^{\frac{3\pi i}{2}}$
χ^2	1	$\mathrm{e}^{\pi i}$	1	$\mathrm{e}^{\pi i}$
χ^3	1	$\mathrm{e}^{\frac{3\pi i}{2}}$	$\mathrm{e}^{\pi i}$	$\mathrm{e}^{\frac{\pi i}{2}}$

$\equiv$

	0	1	2	3
ε	1	1	1	1
χ	1	i	-1	$-i$
χ^2	1	-1	1	-1
χ^3	1	$-i$	-1	i

Si ha

$$\begin{aligned}
&\hat{f}(\varepsilon) = \textstyle\sum_{j=0}^3 f(j)\overline{\varepsilon(j)} = \sum_{j=0}^3 f(j) = 2(i-1)\\
&\hat{f}(\chi) = \textstyle\sum_{j=0}^3 f(j)\overline{\chi(j)} = i + i - i - i = 0\\
&\hat{f}(\chi^2) = \textstyle\sum_{j=0}^3 f(j)\overline{\chi^2(j)} = i + 1 + i + 1 = 2(i+1)\\
&\hat{f}(\chi^3) = \textstyle\sum_{j=0}^3 f(j)\overline{\chi^3(j)} = i - i - i + i = 0
\end{aligned}$$

Quindi, identificando χ^j con j:

	0	1	2	3
$\hat{f}$	$2(i-1)$	0	$2(i+1)$	0

[33] Si noti che questa è esattamente quello che si fa quando si considera $\hat{f} \in L^2(\mathbb{R})$ invece che $f \in L^2(\widehat{\mathbb{R}})$.

Si noti che $\hat{f} \neq 0$ solo nei multipli della frequenza di f (in questo caso, essendo di periodo 2, $\frac{4}{2}$). Si ha:

$$\langle \hat{f}, \hat{f} \rangle = 4[|1-i|^2 + |i+1|^2] = 4 \cdot 4 = 16$$

e

$$\langle f, f \rangle = |i| + |-1| + |i| + |-1 = 4 = \frac{1}{4}\langle \hat{f}, \hat{f} \rangle.$$

L'osservazione dell'esempio precedente riguardo l'insieme su cui $\hat{f} = 0$ vale in generale:

Teorema 5.14. *Siano G un gruppo ciclico finito, d un divisore di $|G|$ e $f : G \to \mathbb{C}$ una funzione tale che $f(a^{d+j}) = f(a^j)$ per ogni j. Sia poi χ_a il generatore di $\widehat{G}$ tale che $\chi_a(a) = e^{\frac{2\pi i}{m}}$. Allora*

$$\hat{f}(\chi_a^k) = 0 \tag{16}$$

per ogni k che non è divisibile per la frequenza $\nu := \frac{|G|}{d}$ di f (in altre parole se $\hat{f}(\chi_a^k) \neq 0$ allora $\nu \mid k$).

Dimostrazione. Poniamo $m = |G|$, $\nu = \frac{m}{d}$ e scriviamo $G = \langle a \rangle = \{e, a, a^2, \dots a^{m-1}\}$. L'insieme $H := \{e, a^d, a^{2d}, \dots a^{(\nu-1)d}\} = \{a^{jd} \mid j = 0, \dots \nu - 1\}$ è un sottogruppo di G. Sia $k \in \mathbb{Z}_m$ un intero che non divide ν e scriviamo $k = p\nu + s$, $0 \leq q < m$, $1 \leq s \leq \nu - 1$. Si ha:

$$\langle f, \chi^k \rangle = \sum_{\ell=0}^{m-1} f(a^\ell)\overline{\chi_a^k(a^\ell)} = \sum_{q=0}^{\nu-1}\sum_{r=0}^{d-1} f(a^{qd+r})\overline{\chi_a^k(a^{qd+r})} = \sum_{q=0}^{\nu-1}\sum_{r=0}^{d-1} f(a^r)\overline{\chi_a^k(a^r)\chi_a^k(a^{qd})}$$
$$= \sum_{q=0}^{\nu-1} \overline{\chi_a^k(a^{qd})} \sum_{r=0}^{d-1} f(a^r)\overline{\chi_a^k(a^r)}.$$

Ora per $0 \leq q \leq \nu - 1$ si ha $a^{qd} \in H$ e $\chi_H^k \neq \varepsilon_H$ perché ν non divide k.[34] Quindi (cfr. Teorema 5.10)

$$\sum_{q=0}^{\nu-1} \overline{\chi_a^k(a^{qd})} = \sum_{h \in H} \overline{\chi_{a|H}^k(h)} = 0. \quad \square$$

Esempio. Sia $f : \mathbb{Z}_8 \to C$ la funzione periodica di periodo 4 (e frequenza 2) definita da

	0	1	2	3	4	5	6	7
f	1	-1	0	2	1	-1	0	2

La tabella dei caratteri di $\mathbb{Z}_8$ è (identificando $\widehat{\mathbb{Z}}_8$ con $\mathbb{Z}_8$ tramite $j \mapsto \chi_1^j$, $\chi_1(1) = \mathrm{e}^{\frac{\pi i}{4}}$):

	0	1	2	3	4	5	6	7
0	1	1	1	1	1	1	1	1
1	1	$\mathrm{e}^{\frac{\pi i}{4}}$	i	$i\mathrm{e}^{\frac{\pi i}{4}}$	-1	$-\mathrm{e}^{\frac{\pi i}{4}}$	$-i$	$-i\mathrm{e}^{\frac{\pi i}{4}}$
2	1	i	-1	$-i$	1	i	1	i
3	1	$i\mathrm{e}^{\frac{\pi i}{4}}$	$-i$	$\mathrm{e}^{\frac{\pi i}{4}}$	-1	$-i\mathrm{e}^{\frac{\pi i}{4}}$	i	$-\mathrm{e}^{\frac{\pi i}{4}}$
4	1	-1	1	-1	1	-1	1	-1
5	1	$-\mathrm{e}^{\frac{\pi i}{4}}$	i	$-i\mathrm{e}^{\frac{\pi i}{4}}$	-1	$\mathrm{e}^{\frac{\pi i}{4}}$	$-i$	$i\mathrm{e}^{\frac{\pi i}{4}}$
6	1	$-i$	-1	i	1	$-i$	-1	i
7	1	$-i\mathrm{e}^{\frac{\pi i}{4}}$	$-i$	$-\mathrm{e}^{\frac{\pi i}{4}}$	-1	$i\mathrm{e}^{\frac{\pi i}{4}}$	i	$\mathrm{e}^{\frac{\pi i}{4}}$

[34] $\chi^k(a^d) = \mathrm{e}^{2\pi i \frac{k}{\nu}} \neq 1$ perché $\nu \not| k$.

e quindi[35]

$$\begin{aligned}
&\hat{f}(0) = 4\\
&\hat{f}(1) = 0\\
&\hat{f}(2) = 2(1-i)\\
&\hat{f}(3) = 0\\
&\hat{f}(4) = 0\\
&\hat{f}(5) = 0\\
&\hat{f}(6) = 2(3+i)\\
&\hat{f}(7) = 0.
\end{aligned}$$

Si noti che $\hat{f}(0), \hat{f}(2), \hat{f}(6) \neq 0$ ma $\hat{f}(4) = 0$ ovvero è possibile che sia $\hat{f}(k) = 0$ anche se $\nu \mid k$.

Concludiamo questo paragrafo con la trasformata di Fourier della convoluzione. Se $f, g : G \to \mathbb{C}$[36] sono due funzioni definiamo convoluzione di f e g la funzione di G in $\mathbb{C}$:

$$f * g : a \mapsto \sum_{b \in G} f(b)g(ab^{-1}).$$

Dato che la funzione $b \mapsto ab$ è una biiezione in G si ha:

$$f * g(a) = \sum_{b \in G} f(b)g(ab^{-1}) = \sum_{c \in G} f(ac^{-1})g(c) = g * f(a)$$

ossia la convoluzione è un'operazione commutativa. Se $f, g, h : G \to \mathbb{C}$ sono tre funzioni si ha:

$$[f * g] * h(a) = \sum_{b \in G} [f * g](b)]h(ab^{-1}) = \sum_{b \in G} \sum_{c \in G} f(c)g(bc^{-1})h(ab^{-1})$$

mentre

$$f * [g * h](a) = \sum_{b \in G} f(b)][g * h](ab^{-1}) = \sum_{b \in G} \sum_{c \in G} f(b)g(c)h(ab^{-1}c^{-1})$$

e scrivendo cb^{-1} invece di c:

$$f * [g * h](a) = \sum_{b \in G} \sum_{c \in G} f(b)g(cb^{-1})h(ac^{-1}) = \sum_{b \in G} \sum_{c \in G} f(c)g(bc^{-1})h(ab^{-1}) = [f * g] * h(a)$$

(avendo scambiato fra loro b e c). Quindi la convoluzione è un'operazione associativa. L'insieme delle funzioni di G in $\mathbb{C}$ con l'operazione $*$ è quindi un gruppoide commutativo.

Esempio. Sia $1_G : G \to \mathbb{C}$, $1_G(a) = 1$ per ogni $a \in G$. Si ha:

$$f * 1_G(a) = \sum_{b \in G} f(b).$$

e quindi in particolare: $1_G * 1_G(a) = |G|$ per ogni $a \in G$.

Teorema 5.15. *Siano $f, g : G \to \mathbb{C}$ due funzioni su un gruppo abeliano finito G. Allora*

$$\widehat{f * g} = \hat{f}\hat{g}. \tag{17}$$

Dimostrazione. Sia $\chi : G \to \mathbb{C}^*$ un carattere su G. Si ha (con $a = bc$):

$$\begin{aligned}
\langle f * g, \chi \rangle &= \sum_{a \in G} f * g(a)\overline{\chi(a)} = \sum_{a \in G} \sum_{b \in G} f(b)g(ab^{-1})\overline{\chi(a)} = \sum_{b \in G} \sum_{c \in G} f(b)g(c)\overline{\chi(bc)}\\
&= \sum_{b \in G} f(b)\overline{\chi(b)} \sum_{c \in G} g(c)\overline{\chi(c)} = \langle f, \chi \rangle \cdot \langle g, \chi \rangle.
\end{aligned}$$

□

[35] I calcoli sono lasciati per esercizio

[36] per evitare confusione denoteremo gli elementi di G con le lettere $a, b, c, \ldots$

6 Il teorema di Dirichlet

Nel 1837 Dirichlet provò il seguente risultato:

Teorema 6.1 (Dirichlet)**.** *Siano a, N interi coprimi (ossia $\gcd(a, N) = 1$). Allora esistono infiniti primi $p \equiv a \mod N$ (ossia la successione $a + kN$, $k \in \mathbb{N}$ contiene infiniti primi).*

Osservazione 6.2. *È chiaro che se $d = \gcd(a, N) > 1$ ogni elemento della successione $\{a + kN\}_{k\in\mathbb{N}}$ è divisibile per d e quindi non è primo. Pertanto la condizione $\gcd(a, N) = 1$ è necessaria perché esistano primi nella successione $\{a + kN\}_{k\in\mathbb{N}}$. Il risultato di Dirichlet dice che se in una successione del tipo $\{a + kN\}_{k\in\mathbb{N}}$ c'è un primo allora ce ne sono infiniti. Supponiamo che $\gcd(a, N) = 1$ e $\gcd(b, N) = 1$. Per $n \in \mathbb{N}$, $x \in \mathbb{N}$ sia $S_{x,n} = \{p = x + kN \leq n \mid p \text{ è primo}\}$ l'insieme dei numeri primi $\leq x$. Un risultato più preciso afferma che*

$$\lim_{n\to\infty} \frac{|S_{a,n}|}{|S_{b,n}|} = 1$$

ossia in ogni successione del tipo $a + kN$ con lo stesso N i numeri primi tendono a distribuirsi (più o meno) uniformemente.

Sia $\mathcal{P}_a = \{p = a + kN \mid p \text{ è primo e } k \in \mathbb{N}\}$. La dimostrazione del Teorema 6.1 consiste nel provare che la serie

$$\sum_{p\in\mathcal{P}_a} \frac{1}{p} \tag{18}$$

è divergente. Da ciò segue subito che in $\mathcal{P}_a$ debbono esserci infiniti elementi altrimenti la serie sarebbe una somma finita e quindi convergente. È utile osservare che il carattere della serie (18) non dipende da come si ordinano i suoi termini dato che $\frac{1}{p} > 0$.[37]

Proveremo il Teorema 6.1 utilizzando l'analisi complessa. Ricordiamo che se $z \in \mathbb{C}$ è un numero complesso di modulo $|z| < 1$ si ha

$$-\log(1 - z) = \sum_{n=1} \frac{z^n}{n}$$

---

[37] Tanto per dare un'idea della difficoltà dell'approccio mostriamo che la serie $\sum_{p\in\mathcal{P}} \frac{1}{p}$ dei reciproci di *tutti* i numeri primi è divergente. Ordiniamo l'insieme dei primi in ordine crescente $\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17, 19, \ldots\}$ e sia p_k il $k-$esimo primo. Così $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$ ecc. Supponiamo, per assurdo, che la serie $\sum_{k=0}^{\infty} \frac{1}{p_k}$ sia convergente. Allora, per ogni $\varepsilon > 0$, esisterebbe N tale che $\sum_{N<k} \frac{1}{p_k} < \varepsilon$. Scegliamo N in modo che $\sum_{N<k} \frac{1}{p_k} < \frac{1}{2}$. Sia $M \in \mathbb{N}$. Scriviamo:

$$\{1, 2, \ldots, M\} = S_1 \cup S_2$$

dove

$$S_1 = \{x \in \mathbb{N} \mid x \leq M \text{ e } p_i \mid x \text{ per qualche } i > N\}$$
$$S_2 = \{x \in \mathbb{N} \mid x \leq M \text{ e } \gcd(p_i, x) = 1 \text{ per ogni } i > N\}$$

Ovviamente $S_1 \cap S_2 = \emptyset$ e quindi $M = |S_1| + |S_2|$. Per ogni elemento $x \in S_2$ possiamo scrivere $x = p_1^{\alpha_1} \cdot \ldots \cdot p_N^{\alpha_N} m^2$, con $\alpha_i = 0, 1$ e $m^2 \leq x \leq M$. Quindi $|S_2| \leq 2^N \sqrt{M}$. Invece per ogni $i > N$ vi sono al più $\frac{M}{p_i}$ numeri naturali $\leq M$ divisibili per p_i ($x = p_i \frac{x}{p_i}$ e $\frac{x}{p_i} \leq \frac{M}{p_i}$). Quindi

$$|S_1| \leq \sum_{i>N} \frac{M}{p_i} \leq \frac{M}{2}.$$

In conclusione

$$M \leq \frac{M}{2} + 2^N \sqrt{M} \Rightarrow \sqrt{M} \leq 2^{N+1}$$

che è assurdo perché N è fissato e invece M è un qualsiasi numero naturale.

Infatti l'uguaglianza vale se $z = x$ è un numero reale di modulo < 1 e quindi vale per $|z| < 1$ per l'unicità del prolungamento analitico. In particolare per ogni funzione $f : \mathbb{C} \to \mathbb{C}$ che soddisfa $|1 - f(z)| < 1$ risulta

$$-\log(f(z)) = -\log(1 - (1 - f(z))) = \sum_{n=1} \frac{(1 - f(z))^n}{n}$$

Sia ora $a \in \mathbb{Z}$ tale che $\gcd(a, N) = 1$. Possiamo supporre $a < N$ e quindi considerare $a \in \mathbb{Z}_N^*$. Vogliamo provare che

$$\sum_{p \in \mathcal{P}_a} \frac{1}{p} = \infty.$$

Per ogni numero complesso s con parte reale $\Re s > 1$ consideriamo la serie convergente[38]

$$\sigma(s) := \sum_{p \in \mathcal{P}_a} \frac{1}{p^s}.$$

L'obiettivo è di provare che $|\sigma(s)|$ è illimitato per $\Re s \to 1^+$. Per semplificare la notazione, d'ora in poi indicheremo con $X = \widehat{\mathbb{Z}_N^*}$, il gruppo dei caratteri su $\mathbb{Z}_N^*$. Sia $\mathcal{P}$ l'insieme dei primi che non dividono N. Si ha ovviamente $p \in \mathcal{P}$ se e solo se p è un numero primo e $\gcd(p, N) = 1$. Per ogni $p \in \mathcal{P}$ scriveremo

$$\chi(p) \text{ in luogo di } \chi(p \mod N).$$

Dal Teorema 5.11 si ottiene, per ogni $p \in \mathcal{P}$:

$$\sum_{\chi \in X} \frac{\chi(a^{-1})\chi(p)}{\varphi(N)} = \begin{cases} 1 & \text{se } p \equiv a \mod N \\ 0 & \text{se } p \not\equiv a \mod N \end{cases}$$

e quindi:

$$\sigma(s) = \sum_{\chi \in X} \frac{\chi(a^{-1})}{\varphi(N)} \sum_{p \in \mathcal{P}} \frac{\chi(p)}{p^s}. \tag{19}$$

Si noti che

$$\sigma(s) = \sum_{p \in \mathcal{P}_a} \frac{1}{p^s} = \sum_{p \in \mathcal{P}_a} \frac{\chi(p)}{p^s}$$

quindi la (19) sembra complicare inutilmente l'espressione di $\sigma(s)$. In realtà la (19) esprime $\sigma(s)$ in un modo *indipendente* da $\mathcal{P}_a$. Nelle prossime righe studieremo la (19) così da distinguerne le parti *convergenti*. Ed è in questa semplificazione che l'analisi complessa ci viene in aiuto. Consideriamo la serie (doppia):

$$\sum_{p \in \mathcal{P}, n \in \mathbb{N}} \frac{1}{n} \left(\frac{\chi(p)}{p^\alpha} \right)^n$$

con $\alpha > 1$. Così come per gli integrali doppi, quando $f(x, y) \geq 0$, il calcolo dell'integrale

$$\iint_{\mathbb{R}^2} f(x, y) dx dy$$

è indipendente dall'ordine di integrazione[39] anche per le serie doppie si ha lo stesso risultato:

---

[38] La serie $\sum_{p \in \mathcal{P}_a} \left| \frac{1}{p^s} \right| = \sum_{p \in \mathcal{P}_a} \frac{1}{p^{\Re s}}$ è a termini positivi e maggiorata dalla serie armonica generalizzata $\sum_{n=1}^{\infty} \frac{1}{n^{\Re s}}$

[39] Nel senso che se uno dei due integrali

$$\int_{-\infty}^{\infty} \left[\int_{-\infty}^{\infty} f(x, y) dx \right] dy \text{ o } \int_{-\infty}^{\infty} \left[\int_{-\infty}^{\infty} f(x, y) dy \right] dx$$

converge, convergono anche l'altro e l'integrale doppio e tutti questi valori sono uguali.

Lemma 6.3. *Sia $\sum_{n,m\in\mathbb{N}} a_{nm}$ una serie con $a_{nm} \geq 0$. Allora se una delle due serie*

$$\sum_{n\in\mathbb{N}} \left[\sum_{m\in\mathbb{N}} a_{nm}\right] \quad \textit{oppure} \quad \sum_{m\in\mathbb{N}} \left[\sum_{n\in\mathbb{N}} a_{nm}\right]$$

converge, converge anche l'altra e si ha:

$$\sum_{n,m\in\mathbb{N}} a_{nm} = \sum_{n\in\mathbb{N}} \left[\sum_{m\in\mathbb{N}} a_{nm}\right] = \sum_{m\in\mathbb{N}} \left[\sum_{n\in\mathbb{N}} a_{nm}\right].$$

Applichiamo il Lemma alla serie (20). Ricordando che, per ogni $z \in \mathbb{C}$ con $|z| \leq 1$ si ha

$$\sum_{n=1}^{\infty} \frac{z^n}{n} = -\log(1-z)$$

vediamo che per ogni $p \in \mathcal{P}$ si ha (con $\alpha = \Re s > 0$):

$$\sum_{n=1}^{\infty} \frac{1}{n}\left(\frac{1}{p^s}\right)^n = -\log\left(1-\frac{1}{p^s}\right)$$

e quindi

$$\sum_{p\in\mathcal{P}} \left[\sum_{n=1}^{\infty} \frac{1}{n}\left|\frac{\chi(p)}{p^s}\right|^n\right] \leq \sum_{p\in\mathcal{P}} \left[\sum_{n=1}^{\infty} \frac{1}{n}\left(\frac{1}{p^\alpha}\right)^n\right] = -\sum_{p\in\mathcal{P}} \log\left(1-\frac{1}{p^\alpha}\right) \simeq \sum_{p\in\mathcal{P}} \frac{1}{p^\alpha} < \infty$$

se $\alpha > 1$. In conclusione, per $\Re s > 1$, e $\chi \in X$, è definita la funzione:

$$\ell(\chi, s) := \sum_{p\in\mathcal{P}, n\in\mathbb{N}} \frac{1}{n}\left(\frac{\chi(p)}{p^s}\right)^n = -\sum_{p\in\mathcal{P}} \log\left(1-\frac{\chi(p)}{p^s}\right). \tag{20}$$

Inoltre $\ell(\chi, s)$ è olomorfa in $\Re s > 1$ perché i singoli addendi lo sono.[40] Poniamo

$$L(\chi, s) = \mathrm{e}^{\ell(\chi,s)} = \prod_{p\in\mathcal{P}} \left(1-\frac{\chi(p)}{p^s}\right)^{-1} \tag{21}$$

Si ha:

$$\ell(\chi, s) = \sum_{p\in\mathcal{P}} \frac{\chi(p)}{p^s} + \sum_{n\geq 2, p\in\mathcal{P}} \frac{1}{n}\left(\frac{\chi(p)}{p^s}\right)^n. \tag{22}$$

e, con $\alpha = \Re s > 1$:

$$\sum_{p\in\mathcal{P}}\sum_{n\geq 2} \frac{1}{n}\left(\frac{|\chi(p)|}{p^\alpha}\right)^n \leq \sum_{p\in\mathcal{P}}\sum_{n\geq 2} \frac{1}{n}\left(\frac{1}{p^\alpha}\right)^n \leq \sum_{p\in\mathcal{P}} -\log\left(1-\frac{1}{p^s}\right) - \frac{1}{p^\alpha} \simeq \sum_{p\in\mathcal{P}} \frac{1}{p^{2\alpha}} < \sum_{n=1}^{\infty} \frac{1}{n^{2\alpha}}$$

che è convergente. Quindi $\displaystyle\sum_{p\in\mathcal{P}} \frac{\chi(p)}{p^s}$ è illimitata per $\Re s \to 1$ se e solo se $\ell(\chi, s)$ è illimitata, per $\Re s \to 1$.

Dalla (19) otteniamo

$$\sigma(s) = \sum_{\chi\in X} \frac{\chi(a^{-1})}{\varphi(N)} \ell(\chi, s) + O(1).$$

e separando il carattere principale dagli altri nella (22):

$$\sigma(s) = \frac{1}{\varphi(N)} \sum_{p\in\mathcal{P}} \frac{1}{p^s} + \sum_{\varepsilon\neq\chi\in X} \frac{\chi(a^{-1})}{\varphi(N)} \ell(\chi, s) + O(1). \tag{23}$$

Allo scopo di studiare la (23) risulta importante il seguente

[40] Teorema di Weierstrass

Teorema 6.4. *Se $\chi \in \widehat{\mathbb{Z}_N^*}$, $\chi \neq \varepsilon$ è un carattere non principale su $\mathbb{Z}_N$ la funzione $L(\chi, s)$ è olomorfa in in un intorno di $s = 1$ e $L(\chi, 1) \neq 0$.*

Non diamo la dimostrazione del Teorema 6.4 che è di carattere puramente analitico e fa intervenire la funzione $\zeta(s)$ di Riemann e le proprietà selle serie di Dirichlet: $\sum_{n=0}^{\infty} \frac{a_n}{n^s}$ con $a_n > 0$. La conseguenza che ci interessa de Teorema 6.4 è la seguente. Assegnato un intorno di $s = 1$ in $\mathbb{C}$ esistono $\delta, M > 0$ tali che

$$\delta < |L(\chi, s)| < M$$

per ogni $\chi \in X$. Possiamo anche supporre che $M\delta > 1$. Quindi, da $\ell(\chi, s) = \log L(\chi, s)$ deduciamo:

$$|\ell(\chi, s)| \leq \log M + 2\pi.$$

Di conseguenza:

$$\sum_{\varepsilon \neq \chi \in X} \frac{\chi(a^{-1})}{\varphi(n)} \ell(\chi, s) = O(1)$$

e

$$\sigma(s) = \frac{1}{\varphi(n)} \sum_{p \in \mathcal{P}} \frac{1}{p^s} + O(1). \tag{24}$$

Dato che in $\mathcal{P}$ ci sono tutti i primi tranne quelli che dividono N (che sono in numero finito), il carattere della serie $\displaystyle\sum_{p \in \mathcal{P}} \frac{1}{p}$ è lo stesso di quello della serie $\displaystyle\sum_{k=1}^{\infty} \frac{1}{p_k}$ dei reciproci di *tutti* i numeri primi che sappiamo essere divergente. Ora siano $s, t \in \mathbb{R}$ tali che $1 < s < t$ Dato che $p_k \geq 2$ si ha $p_k^s < p_k^t$ e quindi

$$\sum_{k=1}^{\infty} \frac{1}{p_k^s} > \sum_{k=1}^{\infty} \frac{1}{p_k^t}$$

Se[41] $\sum_{k=1}^{\infty} \frac{1}{p_k^s}$ fosse limitata, per $s \to 1$, esisterebbe $K \geq 1$ tale che per ogni $n \in \mathbb{N}$:

$$\sum_{k=1}^{n} \frac{1}{p_k^s} < \sum_{k=1}^{\infty} \frac{1}{p_k^s} < K$$

Ma allora anche $\sum_{k=1}^{n} \frac{1}{p_k} \leq K$, per ogni $n \in \mathbb{N}$ e quindi $\sum_{k=1}^{\infty} \frac{1}{p_k} \leq K$ il che è in contraddizione con la divergenza della serie $\displaystyle\sum_{k=1}^{\infty} \frac{1}{p_k}$. Quindi

$$\frac{1}{\varphi(n)} \sum_{p \in \mathcal{P}} \frac{1}{p^s}$$

è illimitata per $s \to 1^+$. Concludendo $\sigma(s)$ è illimitata per $s \to 1$ e quindi $\mathcal{P}_a$ è infinito.

Concludiamo osservando che per ogni $a, b \in \mathbb{Z}_m^*$ si ha:

$$\sum_{p \in \mathcal{P}_a} \frac{1}{p^s} = \frac{1}{\varphi(N)} \sum_{p \in \mathcal{P}} \frac{1}{p^s} + O(1)$$
$$\sum_{p \in \mathcal{P}_b} \frac{1}{p^s} = \frac{1}{\varphi(N)} \sum_{p \in \mathcal{P}} \frac{1}{p^s} + O(1)$$

e quindi

$$\sum_{p \in \mathcal{P}_a} \frac{1}{p^s} - \sum_{p \in \mathcal{P}_b} \frac{1}{p^s} = O(1), \quad \text{per } s \to 1^+.$$

[41] questo ragionamento è la dimostrazione del Lemma di monotonia.

Dividendo per $\sum_{p\in\mathcal{P}_b} \frac{1}{p^s}$ e passando al limite per $s \to 1^+$ si ottiene:

$$\lim_{s\to 1^+} \frac{\sum_{p\in\mathcal{P}_a} \frac{1}{p^s}}{\sum_{p\in\mathcal{P}_b} \frac{1}{p^s}} = 1$$

che è consistente con il fatto che nelle successioni $a + kN$, $a \in \mathbb{Z}_m^*$ la frequenza dei primi è all'incirca la stessa.