CAPITOLO A

Teoria Introduttiva dei Gruppi

Un gruppo è un insieme di elementi munito di una operazione binaria che verifica la proprietà associativa, nel quale esiste un elemento particolare, detto elemento neutro, e in cui ogni elemento ammette il suo inverso.

Quando l'operazione del gruppo verifica anche la proprietà commutativa il gruppo viene chiamato *abeliano*; se inoltre il gruppo è generato da un numero finito di suoi elementi si dice *gruppo abeliano finitamente generato.*

In questo capitolo introdurremo nozioni della teoria dei gruppi, che saranno la base per i capitoli successivi. Indispensabili saranno il teorema di Lagrange, i teoremi di isomorfismo ed il prodotto diretto con la sua caratterizzazione. Infine, alcuni teoremi della teoria dei numeri sono dimostrati come applicazioni esemplari.

A1. Gruppi e sottogruppi

Definizione A1.1. *Sia G un insieme non vuoto munito di un'operazione binaria "$\cdot$". La struttura algebrica $(G, \cdot)$ viene chiamata* gruppo *se gode delle seguenti proprietà:*

(a) Proprietà associativa*: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ per x, y, $z \in G$.*
(b) Elemento neutro*: Esiste $e \in G$ tale che $x \cdot e = e \cdot x = x$ per ogni $x \in G$.*
(c) Inverso*: $\forall x \in G$, esiste un $y \in G$ tale che $x \cdot y = y \cdot x = e$.*

Definizione A1.2. *Sia $(G, \cdot)$ un gruppo. Si dice* $(G, \cdot)$ gruppo finito *se l'insieme G è finito; altrimenti $(G, \cdot)$ viene detto* gruppo infinito.

Definizione A1.3. *Sia $(G, \cdot)$ un gruppo. Si dice* $(G, \cdot)$ gruppo abeliano *se $\forall x, y \in G$ vale la proprietà agguntiva $x \cdot y = y \cdot x$, detta* proprietà commutativa.

Definizione A1.4. *Siano G un gruppo e g un elemento di G. Il più piccolo intero positivo n tale che $g^n = e$ è detto* ordine *di g o anche periodo di g,*

che viene indicato con $o(g) = n$. *Se tale ordine non esiste, si dice* g *di periodo infinito.*

Definizione A1.5. *Un gruppo* $(G, \cdot)$ *è detto* gruppo ciclico *se esiste* $g \in G$ *tale che* $G = \langle g \rangle := \{g^k \mid k \in \mathbb{Z}\}$, *cioè se* G *è generato da un suo elemento. In tal caso, la cardinalità di* G *coincide con l'ordine* $o(g)$ *del generatore* g.

Indichiamo con $\mathbb{N}$ e $\mathbb{N}_0$ rispettivamente l'insieme dei numeri naturali e quello dei numeri interi non negativi. Allora si verifica facilmente che nessuna delle quattro strutture $(\mathbb{N}, +)$, $(\mathbb{N}, \times)$, $(\mathbb{N}_0, +)$ e $(\mathbb{N}_0, \times)$ forma un gruppo. Invece, abbiamo i seguenti gruppi sulla base dei sistemi dei numeri:

- $\mathbb{Z}$ - numeri interi: $(\mathbb{Z}, +)$ è un gruppo ciclico infinito.
- $\mathbb{Q}$ - numeri razionali: $(\mathbb{Q}, +)$ e $(\mathbb{Q}\backslash\{0\}, \times)$ sono gruppi abeliani infiniti.
- $\mathbb{R}$ - numeri reali: $(\mathbb{R}, +)$ e $(\mathbb{R}\backslash\{0\}, \times)$ sono gruppi abeliani infiniti.
- $\mathbb{C}$ - numeri complessi: $(\mathbb{C}, +)$ e $(\mathbb{C}\backslash\{0\}, \times)$ sono gruppi abeliani infiniti.
- $\mathbb{Z}_m$ - l'insieme completo delle classi residue modulo m: $(\mathbb{Z}_m, +)$ è un gruppo ciclico finito.
- $\mathbb{Z}_m^\times$ - l'insieme ridotto delle classi residue modulo m (le classi rappresentate dai primi relativi a m): $(\mathbb{Z}_m^\times, \times)$ è un gruppo abeliano finito.

Definizione A1.6. *Sia* $(G, \cdot)$ *un gruppo. Un sottoinsieme stabile* H *di* G *si dice un* sottogruppo *di* G *se la sottostruttura* $(H, \cdot)$ *è un gruppo.*

NOTAZIONE: Con $H \leq G$ e $H < G$ indichiamo H sottogruppo e sottogruppo proprio di G, rispettivamente.

Per verificare che $(H, \cdot)$ è un gruppo dovremmo prima di tutto controllare che $\forall x, y \in H$, vale $x \cdot y \in H$ dopo di che dimostrare le tre proprietà che caratterizzano la struttura algebrica di gruppo; alternativamente potremmo usare la seguente equivalenza: Se H è un sottoinsieme non vuoto del gruppo G, allora H è un sottogruppo se e solo se per ogni coppia (x, y) di elementi di H anche il prodotto $x \cdot y^{-1}$ appartiene ad H.

Siano G un gruppo, H un sottogruppo di G e x un elemento di G. Definiamo *laterale sinistro* e *laterale destro* di H in G determinati da x rispettivamente come segue:

$$\begin{aligned} xH &= \{xh \mid \forall h \in H\}, \\ Hx &= \{hx \mid \forall h \in H\}. \end{aligned}$$

Ovviamente, laterali destri (sinistri) distinti di H in G sono anche disgiunti e H coincide con il laterale sinistro hH e destro Hh per qualunque $h \in H$.

L'insieme dei laterali sinistri (destri) è una partizione di G. Inoltre, tutti i laterali (sinistri e destri) di H in G sono equipotenti ad H.

Teorema A1.7 (Teorema di Lagrange). *Siano G un gruppo finito e H un suo sottogruppo, allora l'ordine di H divide quello di G.*

DIMOSTRAZIONE. Denotiamo con n il numero dei laterali destri di H in G. Allora $\forall g \in G$, $|Hg| = |H|$, cioè ogni laterale destro è formato da $|H|$ elementi. I laterali destri non sono altro che le classi di equivalenza di G rispetto alla relazione "$\sim$" tale che $\forall x, y \in G$, si ha che

$$x \sim y \iff x \cdot y^{-1} \in H$$

quindi per le proprietà delle relazioni d'equivalenza sappiamo che i laterali sono a due a due disgiunti ed esauriscono G. Allora $|G| = n \cdot |H|$, perciò $|H|$ divide $|G|$. □

Proposizione A1.8 (Gruppo di ordine p). *Sia G un gruppo finito di ordine p, con p primo. Allora G è ciclico.*

DIMOSTRAZIONE. Dato che $|G| = p > 1$, esiste un elemento $g \in G$ tale che $o(g) > 1$. Allora consideriamo il sottogruppo ciclico $H = \langle g \rangle$ generato da g. Secondo il teorema di Lagrange, si ha $1 < |H| = o(g)|p = |G|$, che implica $|H| = o(g) = p$ e $H = G$. Quindi G è un gruppo ciclico. □

A2. Sottogruppi normali e gruppi quozienti

Definizione A2.1. *Siano G un gruppo e H un suo sottogruppo. Se $\forall x \in G$, risulta $Hx = xH$, allora si dice H* sottogruppo normale *di G e si usa la notazione $H \triangleleft G$.*

OSSERVAZIONE: Per $x \in G$, definiamo il coniugato di H sotto x con $H^x := x^{-1}Hx$. Allora per ogni $x \in G$, $xH = Hx$ equivale a $H^x = H$. Perciò H è sottogruppo normale di G se solo se $H^x = H$ per ogni $x \in G$.

Analogamente, per due elementi x e y in un gruppo G, si dice che y è coniugato a x se esiste un $g \in G$ tale che $y = x^g := g^{-1}xg$. Per un fissato $x \in G$, si definisce *classe di coniugio* di x in G come l'insieme di tutti gli elementi coniugati a x in G e si denota con $\mathrm{Cl}(x)$. Allora, H è un sottogruppo normale di un gruppo G se e solo se H contiene tutti i coniugati di tutti suoi elementi.

Per un gruppo G e un suo sottogruppo normale H, possiamo definire l'operazione indotta "$\circ$" per due laterali Hx e Hy come segue:

$$Hx \circ Hy = H \circ xHx^{-1}(xy) = H(xy).$$

Allora per l'insieme dei laterali destri di H in G:

$$G/H \quad = \quad \{Hg \mid g \in G\}$$

abbiamo l'operazione binaria indotta da quella su G:

$$\begin{aligned} \text{“}\circ\text{”}: \quad & G/H \times G/H \longrightarrow G/H; \\ & Hx \circ Hy \quad = \quad H(xy). \end{aligned}$$

Non è difficile vedere che $(G/H, \circ)$ è un gruppo.

Definizione A2.2. *Se G è gruppo e H un sottogruppo normale di G, allora G/H si dice* gruppo quoziente.

A3. Omomorfismo ed isomorfismo

Definizione A3.1. *Siano $(G, \cdot)$ e $(H, \diamond)$ due gruppi. Un'applicazione f da G in H si dice un* omomorfismo *se $f(x \cdot y) = f(x) \diamond f(y)$ per ogni coppia $x, y \in G$. Quando l'applicazione f è iniettiva, suriettiva e biiettiva, l'omomorfismo f viene denominato rispettivamente monomorfismo, epimorfismo e isomorfismo. Nell'ultimo caso, i due gruppi G e H si dicono* isomorfi *e si denotano con $G \cong H$.*

Sia $f : G \longrightarrow H$ un omomorfismo. Si dice nucleo di f e si indica con il simbolo $\ker f$, l'insieme degli elementi di G la cui immagine risulta l'elemento neutro di H. Non è difficile verificare che il nucleo $\ker f$ è un sottogruppo normale di G.

Teorema A3.2 (Primo teorema di omomorfismo). *Siano G e H due gruppi e f un epimorfismo da G ad H. Allora $G/\ker f$ è isomorfo ad H.*

DIMOSTRAZIONE. Per semplicità, denotiamo con $K = \ker f$. Dato che K è un sottogruppo normale di G, allora il gruppo quoziente G/K è ben definito. Consideriamo l'applicazione canonica ϕ indotta da f:

$$\begin{aligned} G/K \xrightarrow{\phi} H \quad & : \quad \phi(Kx) = f(x) \quad \text{per} \quad Kx \in G/K; \\ \phi(Kx \cdot Ky) \quad & = \quad \phi(Kx) \circ \phi(Ky) \quad = \quad f(x) \circ f(y) \\ & = \quad \phi\big(K(x \cdot y)\big) = f(x \cdot y) = f(x) \circ f(y). \end{aligned}$$

Ricordando che f è epimorfismo da G ad H, si ha che ϕ è suriettivo da G/K ad H. Per ogni due laterali Kx e Ky in G/K, se $\phi(Kx) = \phi(Ky)$,

allora $f(x) = f(y)$. Quest'ultima equivale a $f(xy^{-1}) = f(x)f^{-1}(y) = e_H$, dove e_H è l'elemento neutro di H. Dunque abbiamo $xy^{-1} \in K = \ker f$, che implica $Kx = Ky$. Allora ϕ è anche iniettivo, perciò biiettivo. Quindi ϕ è un isomorfismo da G/K ad H. □

Teorema A3.3 (Secondo teorema di isomorfismo). *Sia G un gruppo e siano H e N due sottogruppi normali di G tali che $H \triangleleft N$. Allora il gruppo $\frac{G/H}{N/H}$ è isomorfo a G/N.*

DIMOSTRAZIONE. Consideriamo due epimorfismi canonici:

$$G \xrightarrow{\phi} G/H \quad : \quad \phi(x) = xH \quad \text{per} \quad x \in G;$$
$$G/H \xrightarrow{\psi} \frac{G/H}{N/H} \quad : \quad \psi(xH) = xH(N/H) \quad \text{per} \quad xH \in G/H.$$

Allora l'applicazione composta

$$G \xrightarrow{\psi\diamond\phi} \frac{G/H}{N/H} \; : \; \psi\big(\phi(x)\big) = xH(N/H) \quad \text{per} \quad x \in G$$

è ancora un epimorfismo. Secondo il teorema d'omomorfismo, abbiamo subito che $G/\ker(\psi \diamond \phi)$ è isomorfo a $\frac{G/H}{N/H}$. Rimane da confermare il fatto che $N = \ker(\psi \diamond \phi)$. Infatti, $x \in G$ appartiene a $\ker(\psi \diamond \phi)$ se e solo se $xH(N/H) = N/H$, cioè se e solo se $xH \in N/H$. Quest'ultima è equivalente a $x \in N$. Dunque $N = \ker(\psi \diamond \phi)$ e G/N è isomorfo a $\frac{G/H}{N/H}$. □

Teorema A3.4 (Terzo teorema di isomorfismo). *Sia G un gruppo e siano H ed N rispettivamente un sottogruppo ed un sottogruppo normale di G. Valgono:*

(a) *HN è un sottogruppo di G.*
(b) *N è sottogruppo normale di HN.*
(c) *$HN/N \cong H/(H \cap N)$.*

DIMOSTRAZIONE. Verifichiamo separatamente ognuna di queste tesi.

[a] Osserviamo che HN è sottoinsieme di G perché lo sono sia N che H, inoltre si tratta di un insieme chiuso rispetto a "$\cdot$". Infatti, per due elementi h_1a_1 e h_2a_2 di HN, si nota

$$(h_1a_1) \cdot (h_2a_2) = (h_1h_2) \cdot \big\{(h_2^{-1}a_1h_2) \cdot a_2\big\}$$

appartiene ad HN, perché N è sottogruppo normale di G, quindi si ha $a_1 \cdot h_2 \cdot a_1^{-1} \in N$. Restano da provare le proprietà del gruppo. È ovvio che vale la proprietà associativa perché $HN \subseteq G$. Esiste l'elemento neutro $e \in HN$, lo stesso $e \in G$. Per ogni $ha \in HN$, esiste il suo inverso $a^{-1}h^{-1}$ perché $(ha)^{-1} = a^{-1}h^{-1} = h^{-1}(ha^{-1}h^{-1}) \in HN$.

[b] Osserviamo che N è sottoinsieme di HN perché $N = eN$, inoltre N è sottogruppo normale di G quindi N è sottogruppo normale di HN.

[c] Non è difficile vedere che $H \cap N$ è un sottogruppo normale di H. Consideriamo ϕ la funzione da HN/N in $H/(H \cap N)$ che trasforma, per ogni $ha \in HN$, il generico laterale $haN = hN$ di HN/N in $h(H \cap N) \in H/H \cap N$. Per ogni $h \in H$ e $a \in N$, scriviamo esplicitamente:

$$\phi : HN/N \longrightarrow H/(H \cap N);$$
$$\phi(hN) = \phi(haN) = h(H \cap N).$$

Dimostriamo che ϕ è un isomorfismo.

- ϕ è un omomorfismo. Siano h_1a_1N e h_2a_2N due laterali di HN/N vale che

$$\begin{aligned} &\phi\big((h_1a_1N)\cdot(h_2a_2N)\big) = \phi\big((h_1a_1)\cdot(h_2a_2)N\big) \\ &= \phi\big((h_1h_2)(a_1^{h_2}a_2)N\big) = \phi\big((h_1h_2)N\big) = (h_1h_2)(H \cap N) \\ &= h_1(H \cap N)\cdot h_2(H \cap N) = \phi(h_1a_1N)\cdot\phi(h_2a_2N). \end{aligned}$$

- ϕ è iniettiva. Siano h_1a_1N e h_2a_2N due laterali di HN/N dobbiamo verificare

$$\phi(h_1a_1N) = \phi(h_2a_2N) \implies h_1a_1N = h_2a_2N.$$

Infatti

$$\phi(h_1a_1N) = \phi(h_2a_2N) \implies h_1(H \cap N) = h_2(H \cap N)$$

che implica $h_1h_2^{-1} \in N$, perciò $h_1N = h_2N$ e $h_1a_1N = h_2a_2N$.

- La suriettività è ovvia.

Dunque HN/N è isomorfo a $H/(H \cap N)$. □

A4. Prodotto diretto

Definizione A4.1. *Sia $(G,\cdot)$ un gruppo e siano $H_1, H_2, \cdots, H_n$ sottogruppi di G. Si dice che G è* prodotto diretto *degli $\{H_k\}_{k=1}^n$ se risulta*

(a) *per ogni elemento $g \in G$, si esprime in modo unico come prodotto $g = h_1h_2\cdots h_n$, dove $h_k \in H_k$ per $k = 1, 2, \cdots, n$.*
(b) *ogni elemento di H_i è permutabile con tutti gli elementi di H_j per $i, j = 1, 2, \cdots, n$ con $i \neq j$.*

I gruppi H_k con $k = 1, 2, \cdots, n$ si chiamano fattori diretti *di G. Useremo il seguente simbolo per indicare che G è prodotto diretto degli $\{H_k\}_{k=1}^n$:*

$$G = \bigotimes_{k=1}^{n} H_k = H_1 \otimes H_2 \otimes \cdots \otimes H_n.$$

OSSERVAZIONE: È utile chiarire la precedente definizione:

- La prima proprietà del prodotto diretto dice che ogni elemento g di G si scrive in modo unico come $g = h_1 h_2 \cdots h_n$, il che significa $H_1 H_2 \cdots H_n$ è sottoinsieme di G. Precisa inoltre che $G = H_1 H_2 \cdots H_n$.
- Se G è prodotto diretto dei sottogruppi $H_1, H_2, \cdots, H_n$, non conta l'ordine in cui vengono scritti gli H_i nel prodotto, l'importante è che ognuno di questi compaia una sola volta.
- Se tutti gli H_i sono gruppi abeliani anche G è abeliano.

Teorema A4.2 (Teorema di caratterizzazione). *Siano G un gruppo e $\{H_k\}_{k=1}^n$ sottogruppi di G, allora G è prodotto diretto degli H_k con $k = 1, 2, \cdots, n$ se e solo se*

(a) *tutti gli $\{H_k\}_{k=1}^n$ sono normali.*
(b) $G = \langle H_1, H_2, \cdots, H_n \rangle$.
(c) $\{e\} = H_k \bigcap \langle H_i \mid i \neq k \text{ con } 1 \leq i \leq n \rangle$.

Il sottogruppo $\langle H_1, H_2, \cdots, H_n \rangle$ è generato da $H_1, H_2, \cdots, H_n$, cioè il più piccolo sottogruppo che contiene $H_1, H_2, \cdots, H_n$. Con $\langle H_i \mid i \neq k \rangle$ si indica il sottogruppo generato da tutti gli H_i con $i = 1, 2, \cdots, n$ tranne H_k.

DIMOSTRAZIONE. Supponendo che G sia prodotto diretto degli $\{H_k\}_{k=1}^n$, vogliamo verificare le condizioni necessarie **[a]**, **[b]** e **[c]**.

[a] Dobbiamo dimostrare che, dato $k = 1, 2, \cdots, n$, H_k è sottogruppo normale cioè che

$$\forall g \in G \quad \Longrightarrow \quad H_k^g = g^{-1} H_k g = H_k.$$

Se $g \in G$, sappiamo che esistono $h_i \in H_i$ con $i = 1, 2, \cdots, n$ tali che $g = h_1 \cdot h_2 \cdots h_n$, dove $\{h_i\}_{i=1}^n$ sono due a due permutabili. Osservando che H_k è permutabile con ogni h_i si ha che $H_k^{h_i} = H_k$ con $i \neq k$. Dunque

$$H_k^g = H_k^{h_1 \cdot h_2 \cdots h_n} = H_k^{h_k} = H_k.$$

[b] Dalla definizione di prodotto diretto deriva che $G = \langle H_1, H_2, \cdots, H_n \rangle$.

[c] Dimostriamo che $\forall\ x \in H_k \bigcap \langle H_i \mid i \neq k \rangle\rangle$ risulta $x = e$. Dato che $x \in H_k \bigcap \langle H_i \mid i \neq k \rangle$, esistono $h_j \in H_j$ con $j = 1, 2, \cdots, n$ tali che

$$\begin{aligned} x = \quad h_k \quad &= e \ \cdots e \quad h_k \ e \quad \cdots e \\ &= \prod_{j \neq k} h_j = h_1 \cdots h_{k-1} \ e \ h_{k+1} \cdots h_n. \end{aligned}$$

Per la prima proprietà del prodotto diretto, x ha un'unica fattorizzazione, perciò

$$h_1 = h_2 = \cdots = h_n = e \quad \text{e} \quad x = e.$$

Ora dimostriamo le condizioni sufficienti.

Per ogni $x \in H_i$ e $y \in H_j$ con $i \neq j$, vale $x \cdot y = y \cdot x$.

Siano $x \in H_i$ e $y \in H_j$ generici con $i \neq j$. Osserviamo che:

$$\begin{aligned} x^{-1} \cdot y^{-1} \cdot x \cdot y &= \left(x^{-1} \cdot y^{-1} \cdot x\right) \cdot y \\ &= \left(y^{-1}\right)^x \cdot y \in H_j \end{aligned}$$

dato che $y \in H_j$ e $(y^{-1})^x \in H_j$ perché H_j è un sottogruppo normale.

Analogamente, si ha che

$$\begin{aligned} x^{-1} \cdot y^{-1} \cdot x \cdot y &= x^{-1} \cdot \left(y^{-1} \cdot x \cdot y\right) \\ &= x^{-1} \cdot x^y \in H_i \end{aligned}$$

dato che $x^y \in H_i$ e $x^{-1} \in H_i$ perché H_i è normale.

Quindi

$$x^{-1} \cdot y^{-1} \cdot x \cdot y \in H_i \cap H_j \subseteq H_i \cap \langle H_k \mid k \neq i \rangle = \{e\}$$

perciò $x \cdot y = y \cdot x$, che conferma la proprietà **[b]**.

Dimostriamo che $\forall g \in G$, esistono unici $h_i \in H_i$ con $i = 1, 2, \cdots, n$ tali che $g = h_1 h_2 \cdots h_n$.

Dall'ipotesi **[b]**, si ha che $G = \langle H_1, H_2, \cdots, H_n \rangle$. Conseguentemente abbiamo $G = H_1 \cdot H_2 \cdots H_n$ perché $\{H_k\}_{k=1}^n$ sono a due a due permutabili elemento per elemento.

Resta da provare l'unicità. Sia g un generico elemento di G. Supponiamo che

$$g = h_1 h_2 \cdots h_n = h_1' h_2' \cdots h_n'$$

per $h_k, h'_k \in H_k$ con $k = 1, 2, \cdots, n$. Allora si ottiene che

$$h_1 h_2 \cdots h_n = h'_1 h'_2 \cdots h'_n \quad \Longrightarrow \quad h_k {h'_k}^{-1} = \prod_{\substack{i=1 \\ i \neq k}}^{n} h_i^{-1} h'_i$$

che è giustificato dalla permutabilità dimostrata nella prima parte.

Allora per $k = 1, 2, \cdots, n$ vale

$$h_k {h'_k}^{-1} \in H_k \bigcap \langle \{H_j \mid j \neq k \text{ con } 1 \leq j \leq n\} \rangle = \{e\}.$$

Quindi $h_k {h'_k}^{-1} = e$ che equivale a $h_k = h'_k$ per ogni k con $1 \leq k \leq n$. □

Corollario A4.3. *Siano $\{H_k\}_{k=1}^n$ sottogruppi finiti di un gruppo G a due a due permutabili elemento per elemento. Il loro prodotto è un sottogruppo di G, ed è un prodotto diretto se e solo se ha per ordine il prodotto degli ordini degli H_k con $k = 1, 2, \cdots, n$.*

Notiamo che se per ogni $i = 1, 2, \cdots, n$ si ha H_i finito, allora anche il prodotto $H_1 H_2 \cdots H_n$ è un insieme finito. Se invece gli H_i sono solamente sottogruppi di G, non si può dire che $H_1 H_2 \cdots H_n$ è sottogruppo di G. Però, se $\{H_i\}$ sono sottogruppi finiti del gruppo G a due a due permutabili elemento per elemento, si verifica che $H_1 H_2 \cdots H_n$ è un sottogruppo di G. Infatti:

- $H_1 H_2 \cdots H_n$ è diverso dal vuoto perché $e \in H_i$ per ogni $i = 1, 2, \cdots, n$ quindi $e \in H_1 H_2 \cdots H_n$.
- $H_1 H_2 \cdots H_n$ è sottoinsieme di G (banale).
- Siano $a, b \in H_1 H_2 \cdots H_n$ dimostriamo che ab^{-1} appartiene a $H_1 H_2 \cdots H_n$. Per ogni $i = 1, 2, \cdots, n$ esistono due elementi x_i e y_i appartenenti ad H_i tali che $a = x_1 x_2 \cdots x_n$ e $b = y_1 y_2 \cdots y_n$. Allora:

  $$ab^{-1} = (x_1 x_2 \cdots x_n)(y_1^{-1} y_2^{-1} \cdots y_n^{-1}) = (x_1 y_1^{-1})(x_2 y_2^{-1}) \cdots (x_n y_n^{-1}).$$

DIMOSTRAZIONE. Verifichiamo la condizione necessaria della tesi del corollario. Per ipotesi H è prodotto diretto degli $\{H_k\}_{k=1}^n$, quindi per ogni $h \in H$ esistono $h_i \in H_i$ con $i = 1, 2, \cdots, n$ tali che $h = h_1 h_2 \cdots h_n$. Mostriamo che si deve necessariamente verificare

$$|H| < |H_1| \cdot |H_2| \cdots |H_n| \qquad \text{oppure} \qquad |H| = |H_1| \cdot |H_2| \cdots |H_n|.$$

Infatti, variando nel suddetto prodotto $h_1 h_2 \cdots h_n$ un generico h_k con un altro elemento di H_k, si ottiene un altro elemento di H. Ovviamente h_k può variare in $|H_k|$ modi diversi, quindi, variando tutti gli h_k in tutti i modi possibili, otteniamo $|H_1| \cdot |H_2| \cdots |H_n|$ elementi di H, quindi il numero di

elementi che formano H non può essere inferiore al prodotto delle cardinalità dei vari H_k con $k = 1, 2, \cdots, n$.

Passiamo ora a dimostrare la condizione sufficiente. Per ipotesi

$$H = H_1 H_2 \cdots H_n \quad \text{e} \quad |H| = |H_1| \cdot |H_2| \cdots |H_n|$$

dimostriamo che per ogni $h \in H$ esistono $h_k \in H_k$ con $k = 1, 2, \cdots, n$ tali che $h = h_1 h_2 \cdots h_n$ dove questi h_k sono unici. L'esistenza degli h_k è ovvia in quanto $H = H_1 H_2 \cdots H_n$; resta da provare la loro unicità. Supponiamo per assurdo che esista un elemento $g \in H$ tale che $g = h_1 h_2 \cdots h_n = h_1' h_2' \cdots h_n'$ con almeno un indice k tra questi n tale che $h_k \neq h_k'$. Allora g scritto in due modi diversi contribuisce una volta in $|H_1 H_2 \cdots H_n|$ e due volte in $|H_1| \cdot |H_2| \cdots |H_n|$ per cui $|H_1 H_2 \cdots H_n| < |H_1| \cdot |H_2| \cdots |H_n|$ il che è assurdo! □

A5. Applicazione alla teoria dei numeri

A5.1. Il piccolo teorema di Fermat. Sia p un primo. Denotiamo con $\mathbb{Z}_p^\times$ l'insieme dei residui modulo p diversi da zero. Dimostrare:

(a) $\mathbb{Z}_p^\times$ è un gruppo con la moltiplicazione modulare.
(b) per ogni numero intero n, vale $n^p \equiv n \pmod{p}$.

DIMOSTRAZIONE. Prima di tutto, è facile vedere che $1 \in \mathbb{Z}_p^\times$ è l'elemento neutro di $\mathbb{Z}_p^\times$. Per due elementi $m,\ n \in \mathbb{Z}_p^\times$, il loro prodotto modulo p è diverso da zero, quindi appartiene ancora a $\mathbb{Z}_p^\times$. Perciò $\mathbb{Z}_p^\times$ è chiuso rispetto alla moltiplicazione modulare. Per ogni intero $m \in \mathbb{Z}_p^\times$, consideriamo $M = \{m, m^2, \cdots, m^p\}$, p-interi generati dalle potenze di m. Dato che la cardinalità di $\mathbb{Z}_p^\times$ è uguale a $p-1$, allora esistono due numeri m^i e m^j in M con $1 \leq i < j \leq p$ tali che $m^i \equiv m^j \pmod{p}$. Notando che $\mathrm{mcd}(m, p) = 1$ e $\mathrm{mcd}(m^i, p) = 1$, possiamo subito dedurre che

$$m^{j-i} = m \times m^{j-i-1} \equiv 1 \pmod{p}.$$

Questa congruenza significa che m^{j-i-1} è inverso di m in $\mathbb{Z}_p^\times$. È ovvio che $\mathbb{Z}_p^\times$ è commutativo e anche associativo. Dunque $\mathbb{Z}_p^\times$ è un gruppo abeliano di ordine $p-1$.

Per qualunque numero intero n, se $p|n$, abbiamo

$$n^p \equiv n \equiv 0 \pmod{p}.$$

Altrimenti, consideriamo il sottogruppo $\langle n \rangle$ di $\mathbb{Z}_p^\times$ generato da n. Secondo il teorema di Lagrange, l'ordine d di $\langle n \rangle$ è un divisore dell'ordine di $\mathbb{Z}_p^\times$, che implica

$$n^{p-1} = \left(n^d\right)^{(p-1)/d} \equiv 1 \pmod{p}.$$

Moltiplicado con n, otteniamo in questo caso la stessa congruenza

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

Così abbiamo dimostrato il piccolo teorema di Fermat tramite la teoria dei gruppi finiti. □

A5.2. Funzione Eulero. Per un numero naturale m, sia $\Phi(m)$ l'insieme degli interi da 1 a m, primi relativi a m.

(a) Dimostrare che $\Phi(m)$ è un gruppo con la moltiplicazione modulare rispetto a m.
(b) *Teorema Eulero*: Per ogni intero k con $\mathrm{mcd}(k, m) = 1$, dimostrare la congruenza $k^{\varphi(m)} \equiv 1 \pmod{m}$ dove $\varphi(m)$ è la funzione di Eulero.
(c) Per $n > 1$ un altro numero naturale, dimostrare che m divide $\varphi(n^m - 1)$.

DIMOSTRAZIONE. Seguendo la stessa procedura della dimostrazione del piccolo teorema di Fermat, possiamo confermare che $\Phi(m)$ è veramente un gruppo con la moltiplicazione modulare rispetto a m ed il teorema Eulero

$$k^{\varphi(m)} \equiv 1 \pmod{m} \quad \text{se} \quad \mathrm{mcd}(k, m) = 1.$$

Per l'affermazione (c), consideriamo il sottogruppo $\langle n \rangle$ di $\Phi(n^m - 1)$ generato da n. Non è difficile verificare $\langle n \rangle = \{1, n, n^2, n^{m-1}\}$, che implica $|\langle n \rangle| = m$. Allora $m | \varphi(n^m - 1)$, in virtù del teorema di Lagrange. □

A5.3. Funzione Eulero ancora. Sia G un gruppo ciclico. Dimostrare le seguenti affermazioni:

(a) Ogni sottogruppo H di G è ciclico. Determinare il numero dei generatori di H.
(b) Se G è finito con $|G| = m < \infty$, allora per ogni $n | m$, esiste un solo sottogruppo di ordine n in G.
(c) La formula della somma finita $m = \sum_{n|m} \varphi(n)$, dove φ è la funzione di Eulero.

DIMOSTRAZIONE. Se $G = \langle g \rangle$ è infinito, allora G è isomorfo a $(\mathbb{Z}, +)$ e quindi ha solo due generatori g e g^{-1}. Se $G = \langle g \rangle$ invece è finito con l'ordine $|G| = m$, allora il numero dei generatori è uguale a $\varphi(m)$. Infatti,

se g^k è un qualunque generatore di G, allora $\mathrm{mcd}(k,m) = 1$. Altrimenti, $\mathrm{mcd}(k,m) > 1$ ci porterebbe alla seguente espressione:

$$m = o(g^k) = \left|\{g^k, g^{2k}, \cdots, g^{k\times\frac{m}{\mathrm{mcd}(k,m)}}\}\right| \leq \frac{m}{\mathrm{mcd}(k,m)} < m.$$

Quindi ogni generatore g^k di G corrisponde a un numero naturale k con $1 \leq k \leq m$ tale che $\mathrm{mcd}(k,m) = 1$. Perciò il numero dei generatori del gruppo G è proprio uguale alla funzione Eulero $\varphi(m)$.

[a] Sia $G = \langle g\rangle$ un gruppo ciclico generato da g. Per un sottogruppo $H < G$, consideriamo l'elemento g^n di H come minima potenza positiva di g. Allora $H = \langle g^n\rangle$. Altrimenti, esiste un numero intero positivo k con $n\nmid k$, tale che $g^k \in H$. Secondo l'algoritmo di Euclide, esistono due interi q e r con $0 < r < n$ tali che $k = nq + r$. Allora troviamo un elemento

$$g^r = g^k \cdot \left(g^n\right)^{-q} \in H$$

che contraddice il fatto che g^n sia l'elemento di H con minima potenza positiva di g. Quindi H è ciclico.

Quando G è infinito, generato da g, è facile vedere che ogni sottogruppo $H = \langle g^n\rangle$ è infinito ed ha solo due generatori g^n e g^{-n}. Invece, se G è finito con $|G| = m$, allora H pure è finito. Supponendo che $|H| = n$, si ha che il numero dei generatori di H è uguale a $\varphi(n)$.

[b] Per ogni divisore $n|m$, è evidente che il sottogruppo ciclico

$$H := \langle g^{\frac{m}{n}}\rangle = \left\{g^{\frac{m}{n}}, g^{\frac{2m}{n}}, \cdots g^{\frac{(n-1)m}{n}}, g^m = e\right\}$$

ha ordine n. Vogliamo verificare che, fissando l'ordine n, questo è l'unico sottogruppo di G.

Ricordando che per $G = \langle g\rangle$, ogni sottogruppo ciclico di ordine n è generato da qualche g^k con $o(g^k) = n$, se proviamo che $g^k \in H$, allora H è l'unico sottogruppo di ordine n in G.

Dato che $o(g^k) = n$, si ha che $g^{kn} = e$. Allora esiste un numero naturale d tale che $kn = md$ perché $o(g) = m$. Da questo possiamo dedurre:

$$g^k = g^{md/n} = \left(g^{\frac{m}{n}}\right)^d \in H.$$

Dunque, per ogni $n|m = |G|$, esiste un solo sottogruppo ciclico di ordine n.

[c] Ora, ogni elemento di G è generatore di qualche sottogruppo di G e vice versa, ogni sottogruppo H ha i generatori in numero $\varphi(|H|)$. Classificando

i generatori (tutti gli elementi di G) secondo l'ordine dei sottogruppi di G, otteniamo la seguente formula:

$$m = |G| = \sum_{H \leq G} \varphi(|H|) = \sum_{n|m} \varphi(n).$$

Così abbiamo completato la soluzione del problema. □

A5.4. Teorema di Wilson. Se G è un gruppo abeliano finito con $G = \{g_k\}_{k=1}^n$, dimostrare che $\prod_{k=1}^n g_k$ è un elemento di G il cui quadrato è l'elemento neutro.

(a) Se il gruppo G non ha elementi di ordine 2, dimostrare che $\prod_{k=1}^n g_k = e$ (l'elemento neutro).
(b) Se il gruppo G ha un solo elemento x di ordine 2, dimostrare che $\prod_{k=1}^n g_k = x$.
(c) (Teorema di Wilson) Per un numero primo p, dimostrare la congruenza

$$(p-1)! \equiv -1 \pmod{p}.$$

DIMOSTRAZIONE. Consideriamo un automorfismo su G definito da

$$\psi : G \longrightarrow G \quad \text{con} \quad \psi(x) = x^{-1} \quad \text{per} \quad x \in G.$$

Allora si ha che

$$g = \prod_{k=1}^{n} g_k = \prod_{k=1}^{n} g_k^{-1} = g^{-1}$$

che implica $g^2 = e$, l'elemento neutro di G.

Se $G = \{g_k\}_{k=1}^n$ ha un solo elemento di ordine 2, allora $\{g_1, g_2, \cdots, g_n\}$ possono essere raggruppati in coppie di elementi reciproci più l'elemento neutro e ed un elemento x di ordine 2. Allora si ha che

$$g = \prod_{k=1}^{n} g_k = e \cdot x = x.$$

Ricordiamo che $\mathbb{Z}_p^\times$, l'insieme ridotto dei residui modulo p, è un gruppo abeliano di ordine $p-1$ (in più, $\mathbb{Z}_p^\times$ è ciclico) co la moltiplicazione modulare rispetto a p. Evidentemente $p-1$ è un elemento di ordine 2 in $\mathbb{Z}_p^\times$. Non ci sono altri elementi di ordine 2 in $\mathbb{Z}_p^\times$. Infatti, supponiamo che esista un $k \in \mathbb{Z}_p^\times$ tale che $k^2 \equiv 1 \pmod{p}$. Allora $k \equiv \pm 1 \pmod{p}$, in cui il segno "+" corrisponde all'elemento neutro mentre quello "−" a $p-1$. Dunque

$$(p-1)! \equiv p-1 \equiv -1 \pmod{p}$$

che è il teorema di Wilson. □

A5.5. Numeri armonici: Teorema di Wolstenholme. Per un primo dispari p, si definisce la somma parziale

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1} \;=\; \frac{m}{n}$$

dove m e n sono numeri naturali. Dimostrare che $p|m$. Inoltre se $p>3$, si ha che $p^2|m$.

DIMOSTRAZIONE. Consideriamo di nuovo il gruppo $\mathbb{Z}_p^\times$, l'insieme ridotto dei residui modulo p co la moltiplicazione modulare rispetto a p. Definiamo un automorfismo su $\mathbb{Z}_p^\times$ come segue:

$$\psi:\ \mathbb{Z}_p^\times \longrightarrow \mathbb{Z}_p^\times \quad \text{con} \quad \psi(k)=k^{-1} \quad \text{per} \quad k\in\mathbb{Z}_p^\times.$$

Scriviamo la somma armonica come segue:

$$\frac{m}{n} \;=\; \sum_{k=1}^{p-1}\frac{1}{k} \;=\; \frac{S(p)}{(p-1)!} \quad \text{dove} \quad S(p):=\sum_{k=1}^{p-1}\frac{(p-1)!}{k}.$$

Per dimostrare $p|m$, è sufficiente verificare che p divide $S(p)$.

Secondo il teorema di Wilson, si ha che

$$\begin{aligned} S(p) \;&=\; \sum_{k=1}^{p-1}\frac{(p-1)!}{k} \;\equiv_p\; -\sum_{k\in\mathbb{Z}_p^\times} k^{-1} \\ &\equiv_p\; -\sum_{k\in\mathbb{Z}_p^\times} k \;\equiv_p\; -\binom{p}{2} \;\equiv_p\; 0 \end{aligned}$$

che significa $p|S(p)$, da cui si deduce $p|m$.

Per $p>3$, possiamo riformulare la somma $S(p)$ come segue:

$$\begin{aligned} S(p) \;=\; \sum_{k=1}^{p-1}\frac{(p-1)!}{k} \;&=\; \sum_{k=1}^{(p-1)/2}\left\{\frac{(p-1)!}{k}+\frac{(p-1)!}{p-k}\right\} \\ &=\; p\sum_{k=1}^{(p-1)/2}\frac{(p-1)!}{k(p-k)}. \end{aligned}$$

Per dimostrare $p^2|m$, dobbiamo verificare che p divide la somma destra.

Per il sottogruppo $\mathbb{Z}_p^{\times 2}$ composto dai quadrati degli elementi di $\mathbb{Z}_p^{\times}$, ψ induce pure un automorfismo. Allora possiamo procedere come segue:

$$\sum_{k=1}^{(p-1)/2} \frac{(p-1)!}{k(p-k)} \equiv_p \sum_{k\in\mathbb{Z}_p^{\times 2}} k^{-1} \equiv_p \sum_{k\in\mathbb{Z}_p^{\times 2}} k$$

$$\equiv_p \sum_{k=1}^{(p-1)/2} k^2 \equiv_p \frac{p(p^2-1)}{24}.$$

Notando che $p \equiv \pm 1 \pmod 6$, si ha che $24|(p^2-1)$. Conseguentemente, la frazione destra è un intero che è multiplo di p. Dunque $p^2|m$ per $p > 3$. $\square$