1 GRUPPI

Definizione 1.1.

Sia G un insieme, $G \neq \varnothing$ e sia $*$ un'operazione su G. Si dice che $(G, *)$ è un **gruppo** se

1. $*$ è associativa, ossia $\forall a, b, c \in G, \quad (a * b) * c = a * (b * c)$.
2. Esiste un elemento neutro, ossia $\exists e \in G$ tale che $g * e = e * g = g \ \ \forall g \in G$.
3. Esiste l'inverso di ogni el., ossia: $\forall g \in G \quad \exists g^{-1} \in G$ tale che $g * g^{-1} = g^{-1} * g = e$.

Definizione 1.2.

Un gruppo $(G, *)$ si dice **abeliano** se $*$ è commutativa, cioè $\forall g, h \in G, \quad g * h = h * g$.

Osservazione 1.3.

Per verificare che un insieme non vuoto è un gruppo occorre fare anche la verifica che $*$ sia un'operazione su G, cioè che $\forall g, h \in G \ \ g * h \in G$

Esempio 1.4.

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sono gruppi abeliani rispetto alla somma $+$
2. $(\mathbb{N}, +)$ non è un gruppo.
3. $(\mathbb{Z}, \cdot)$ non è un gruppo.
4. $(\mathbb{Q}^*, \cdot)$ è un gruppo.
5. $(\{x \in \mathbb{C} \mid x^n = 1\}, \cdot)$ è un gruppo.
6. $(\{f : X \longrightarrow X \mid f \text{ è bigettiva}\}, \circ)$ è un gruppo.
7. $(\mathbb{Z}/m\mathbb{Z}, +)$ è un gruppo.
8. $\cdot$ è un'operazione su $\mathbb{Z}/m\mathbb{Z}$ ma $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ non è un gruppo.
9. $(\mathbb{Z}/m\mathbb{Z}^*, \cdot)$ è un gruppo per ogni m.

Notazione 1.5.

Nel seguito ometteremo il simbolo di operazione tra elementi di G, cioè al posto di $a * b$ scriveremo semplicemente ab

Poniamo inoltre $a^0 = e$ e

$\forall n \in \mathbb{N}_{>0}$ poniamo $a^n = \overbrace{a \cdot \cdots \cdot a}^{n \text{ volte}}$ e $\forall n \in \mathbb{N}$ e $a^{-n} = \overbrace{a^{-1} \cdot \cdots \cdot a^{-1}}^{n \text{ volte}}$

Proposizione 1.6.

Sia G un gruppo. Allora

1. l'elemento neutro di G è unico;
2. ogni $a \in G$ ha un unico inverso in G;
3. $\forall a \in G,\ (a^{-1})^{-1} = a$;
4. $\forall a, b \in G,\ (ab)^{-1} = b^{-1}a^{-1}$;
5. valgono le due **leggi di cancellazione**:
   $\forall a, b, c \in G,\ ab = ac \iff b = c$
   $ba = ca \iff b = c$

DIMOSTRAZIONE.

1. Siano e ed e' due elementi neutri di G. Allora $e * e' = e'$ perché e è l'elemento neutro ma vale anche $e * e' = e$ perché e' è l'elemento neutro. Quindi $e = e'$
2. Siano $a \in G$ e siano $x, y \in G$ due suoi inversi, allora: $xa = ax = e$ e $ay = e$ $\Rightarrow$ $y = (xa)y = x(ay) = xe = x$.
3. Segue dal punto 2 osservando che $a * a^{-1} = a^{-1} * a = e$ cioè che a verifica le proprietà dell'inverso di a^{-1}.
4. $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$ che può essere riscritta come $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$.
   Quindi $b^{-1}a^{-1}$ è l'inverso di ab.
5. $ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac) \Rightarrow (a^{-1}a)b = (a^{-1}a)c \Rightarrow b = c$.
   Viceversa se $b = c$ allora $ab = ac$.

   Analogamente si dimostra l'altra condizione

▲

Definizione 1.7.

Sia G un gruppo e sia $H \subset G$ con $H \neq \varnothing$.
H si dice **SOTTOGRUPPO** di G ($H < G$) se H è un gruppo con l'operazione indotta dall'operazione di G.

Proposizione 1.8.

Sia $H \subset G$, $H \neq \varnothing$. Allora $H < G$ se e solo se

1. $\forall a, b \in H \;\; ab \in H$
2. $\forall a \in H \;\; a^{-1} \in H$

DIMOSTRAZIONE.

" $\Rightarrow$ " ovvio.

" $\Leftarrow$ " l'operazione è associativa perché lo è in G .

$H \neq \varnothing \;\Rightarrow\; \exists a \in H$, allora per la condizione 2 si ha che $a^{-1} \in H$, e quindi per la condizione 1 si ha $a^{-1}a = e \in H$. ▲

Esempio 1.9.

1. Sia G un gruppo, allora G e $\{e\}$ sono sottogruppi.
2. Sia G un gruppo e sia $Z(G) := \{x \in G \mid xy = yx \;\forall y \in G\}$ (=**centro di** G). $Z(G)$ è un sottogruppo di G . Infatti
   - $e \in Z(G)$:
   - $\forall x_1, x_2 \in Z(G) \;\; (x_1x_2)y = x_1(x_2y) =$
     $$= (x_1y)x_2 = y(x_1x_2) \;\Rightarrow\; x_1x_2 \in Z(G)$$
   - $\forall x \in Z(G) \;\; xy = yx \;\forall y \in G$ moltiplicando a sinistra e a destra per x^{-1} si ottiene
     $$yx^{-1} = x^{-1}xyx^{-1} = x^{-1}yxx^{-1} = x^{-1}y$$
     quindi $x^{-1} \in Z(G)$.
3. Per ogni $n \in \mathbb{Z}$
   $$n\mathbb{Z} := \{nx \mid x \in \mathbb{Z}\}$$
   è un sottogruppo di $\mathbb{Z}$.

Proposizione 1.10.

$\forall H, K < G,\ H \cap K < G.$

DIMOSTRAZIONE.

- $e \in H \cap K$
- $\forall x, y \in H \cap K\ xy \in H,\ xy \in K \ \Rightarrow\ xy \in H \cap K$
- $\forall x \in H \cap K\ x^{-1} \in H,\ x^{-1} \in K \ \Rightarrow\ x^{-1} \in H \cap K$ ▲

Osservazione 1.11.

In generale $H \cup K$ non è un sottogruppo. Ad esempio $2\mathbb{Z} \cup 3\mathbb{Z}$ non è un sottogruppo di $\mathbb{Z}$.

GRUPPI CICLICI. Ordine di un elemento

Sia G un gruppo, e sia $x \in G$. Poniamo

$$< x >:= \{x^m\}_{m \in \mathbb{Z}}$$

Proposizione 1.12.

$\forall x \in G$ si ha $< x >< G$

DIMOSTRAZIONE.

- $< x > \subset G$ perché $x \in G \ \Rightarrow\ x^{-1} \in G$ e quindi, essendo G chiuso rispetto al prodotto, $x^n \in G \forall n \in \mathbb{Z}$.
- $e = x^0 \in < x >$.
- $\forall x^m, x^n \in < x > \ \Rightarrow\ x^m x^n = x^{m+n} \in < x >$.
- Sia $x^m \in < x >$, allora $(x^m)^{-1} = x^{-m} \in < x >$.

▲

$< x >$ si dice **sottogruppo generato da** x . Osserviamo che $< x >$ è abeliano.

Osservazione 1.13.

Sia $x \in G$, se le potenze di x sono tutte distinte allora $< x >$ è infinito.

Se invece $\exists m, n \ (m > n)$ tali che $x^m = x^n$ allora $x^{m-n} = e$.

Da questo segue che le potenze di x si ripetono ciclicamente: infatti, se

$x^{m-n} = e$ allora $x^{m-n+1} = x$ e così via e quindi $< x >$ è finito.

Definizione 1.14.

Sia $x \in G$. Si definisce ordine dell'elemento x :

$$\mathrm{ord}_G(x) := \min\{k > 0 \mid x^k = e\}$$

con la convenzione che $\min \varnothing = +\infty$.

Si dice ordine di un gruppo la sua cardinalità.

Proposizione 1.15.

Sia $x \in G$ con $\mathrm{ord}(x) = d < +\infty$. Allora

$$< x >= \{e, x, \ldots, x^{d-1}\}$$

e $\# < x >= d$.

Inoltre se $x^n = e \ \Rightarrow \ d \mid n$.

Dimostrazione.

Pioché ovviamente $\{e, x, \ldots, x^{d-1}\} \subseteq < x >$, basta vedere che $\forall m \in \mathbb{Z}$ si ha $x^m \in \{e, x, \ldots, x^{d-1}\}$.

Sia $m = qd + r$ con $0 \leq r < d$. Poiché $x^d = e$ si ha

$$x^m = x^{qd+r} = (x^d)^q x^r = e x^r = x^r \in \{e, x, \ldots, x^{d-1}\}$$

Gli elementi $\{e, x, \ldots, x^{d-1}\}$ sono tra loro distinti poiché se fosse $x^i = x^j$ con $0 \leq i < j < d$ avremmo $x^{j-i} = e$ ma $0 < j - i < d = \mathrm{ord}(x)$ e questo è assurdo.

Infine se $x^n = e$ e se $n = qd + r \ \Rightarrow \ e = x^n = (x^d)^q x^r = x^r$.

Per la minimalità di d si deve avere $r = 0, ;$ cioè $d \mid n$

▲

Definizione 1.16.

Un gruppo G si dice **ciclico** se $\exists x \in G$ tale che $G =< x >$.

Esempio 1.17.

1. $\mathbb{Z} =< 1 >$ è un gruppo ciclico infinito
2. $n\mathbb{Z} =< n >$ è un sottogruppo ciclico infinito di $\mathbb{Z}$ per ogni $n \in \mathbb{Z}$
3. $\mathbb{Z}/n\mathbb{Z} =< [1]_n >$ è un gruppo ciclico di ordine n.

Teorema 1.18.

Ogni sottogruppo di un gruppo ciclico è ciclico.

Dimostrazione.

Sia $G =< g >$ e sia $H < G$. Se $H =< e >$ allora H è ciclico.
Supponiamo quindi che $\exists k \geq 1$ tale che $g^k \in H$.
Sia $I := \{k \in \mathbb{N} \mid g^k \in H\} \subset \mathbb{N}$ e sia

$$S := I \cap \mathbb{N}_{>0}.$$

Per quanto detto $S \neq \varnothing$, quindi ammette un minimo h.
Dimostriamo che $H =< g^h >$.
Infatti $< g^h > \subset H$ perché $g^h \in H$ e H è un sottogruppo.
Viceversa sia $g^k \in H$ e sia

$$k = qh + r \quad 0 \leq r < h \quad \Rightarrow \quad g^k \cdot (g^h)^{-q} = g^r \in H$$

Per la limitazione su r e la minimalità di h segue che $r = 0$,
ossia $g^k \in < g^h >$. ▲

Corollario 1.19 (Sottogruppi di $\mathbb{Z}$)**.**

Sia $H < \mathbb{Z}$, allora $\exists n \in \mathbb{N}$ tale che $H = n\mathbb{Z}$.

Dimostrazione.

Poicé $\mathbb{Z}$ è ciclico il teorema precedente ci assicura che i suoi sottogruppi sono tutti ciclici, cioè del tipo $H =< n >= n\mathbb{Z}$ con $n \in \mathbb{Z}$. Poichè $-n\mathbb{Z} = n\mathbb{Z}$ si ha la tesi. ▲

Esercizio 1.20.

Provare che $n\mathbb{Z} \cap m\mathbb{Z} = [n, m]\mathbb{Z}$

Il gruppo $\mathbb{Z}/n\mathbb{Z}$.

Abbiamo già osservato che $(\mathbb{Z}/n\mathbb{Z}, +)$ è un gruppo abeliano. Questo gruppo è anche ciclico perché $\mathbb{Z}/n\mathbb{Z} =< [1]_n >$.

Proposizione 1.21. Per ogni classe $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ si ha

$$\text{ord}[a]_n = \frac{n}{(a, n)}.$$

Da questo segue che:

1. $\mathbb{Z}/n\mathbb{Z}$ ha $\Phi(n)$ elementi di ordine n e questi sono precisamente $[a]_n$ con $(a, n) = 1$ (questi elementi sono i generatori di $\mathbb{Z}/n\mathbb{Z}$ come gruppo ciclico).
2. $\forall\, [a]_n \in \mathbb{Z}/n\mathbb{Z}$ si ha $\text{ord}[a]_n \mid n$.
3. $\forall d \mid n$ esistono esattamente $\Phi(d)$ elementi di $\mathbb{Z}/n\mathbb{Z}$ di ordine d .
4. Sottogruppi di $\mathbb{Z}/n\mathbb{Z}$. Sia $H < \mathbb{Z}/n\mathbb{Z}$. Allora H è ciclico e $|H| = d$ per un certo $d \mid n$.

   Viceversa se per ogni $d \mid n$ esiste un unico sottogruppo H_d di $\mathbb{Z}/n\mathbb{Z}$ di ordine d , e si ha $H_d =< [\frac{n}{d}]_n >$.

Dimostrazione.

Per definizione $\text{ord}[a]_n = \min\{k > 0 \mid k[a]_n = [0]_n\}$, cerco quindi la minima soluzione positiva di

$$ax \equiv 0 \ \ (n).$$

Tale equazione è equivalente a

$$x \equiv 0 \quad \left(\frac{n}{(a, n)}\right),$$

da cui otteniamo $\text{ord}[a] = \ \frac{n}{(a,n).}$

In particolare si ha che $\text{ord}[a] = n \Leftrightarrow (a, n) = 1 \Leftrightarrow [a] \in \mathbb{Z}/n\mathbb{Z}^*$. Quindi:

1. Segue dalla formula trovata.
2. Segue anch'esso dalla formula precedente.
3. $\text{ord}[a] = \frac{n}{(a,n)} = d \Leftrightarrow (a, n) = \frac{n}{d} \Leftrightarrow a = \frac{n}{d}b$ con $(b, d) = 1$ e $1 \leq b \leq d$.

   Gli elementi a di ordine d sono quindi $\Phi(d)$.

4. Poiché $\mathbb{Z}/n\mathbb{Z}$ è un gruppo ciclico tutti i suoi sottogruppi sono ciclici.

   Sia $H =< [a] >$, allora $|H| = \text{ord}[a]$ e quindi $|H| \mid n$.

   Viceversa sia $d \mid n$ e sia

$$H_d =< \left[\frac{n}{d}\right]_n >= \{[0], \left[\frac{n}{d}\right], \left[\frac{2n}{d}\right], \ldots, \left[\frac{n}{d}\,(d-1)\right]\}$$

   È semplice verificare che H_d è un sottogruppo di ordine d e che contiene tutti gli elementi di ordine d di $\mathbb{Z}/n\mathbb{Z}$.

   Ne segue che ogni elemento di ordine d di $\mathbb{Z}/n\mathbb{Z}$ genera H_d.

▲

Corollario 1.22. Per ogni $n \geq 1$ si ha $n = \sum_{d|n} \Phi(d)$.

DIMOSTRAZIONE.

Sia $X_d = \{[a]_n \in \mathbb{Z}/n\mathbb{Z} \mid \text{ord}[a]_n = d\}$.

La proposizione precedente assicura che

$$|X_d| = \begin{cases} \Phi(d) & d \mid n \\ 0 & \text{altrimenti} \end{cases}$$

Poiché $\mathbb{Z}/n\mathbb{Z} = \overset{\circ}{\bigcup_{d \mid n}} X_d$, passando alle cardinalità si opttiene $n = \sum_{d|n} \Phi(d)$. ▲

Omomorfismi.

Definizione 1.23.

Siano $(G, *)$ e $(G', *')$ due gruppi. Una funzione $f : G \longrightarrow G'$ si dice **omomorfismo** se

$$\forall x, y \in G, \quad f(x * y) = f(x) *' f(y)$$

Proposizione 1.24. Sia $f : G \longrightarrow G'$ omomorfismo. Allora

1. $f(e) = e'$;
2. $f(x^{-1}) = (f(x))^{-1}$;
3. $H < G \Rightarrow f(H) < G'$;
   $K < G' \Rightarrow f^{-1}(K) < G$;

4. $f(G) < G'$ e $\operatorname{Ker} f := \{x \in G \mid f(x) = e'\} < G$
5. f è iniettivo $\iff$ $\operatorname{Ker} f = \{e\}$

DIMOSTRAZIONE.

1. $f(e) = f(ee) = f(e)f(e)$. La legge di cancellazione assicura che $f(e) = e'$.
2. $\forall x \in G\, e' = f(e) = f(xx^{-1}) = f(x)f(x^{-1})$
   ed inoltre $e' = f(e) = f(x^{-1}x) = f(x^{-1})f(x)$
   cioè $f(x^{-1})$ è l'inverso di $f(x)$
   Poichè $H \neq \varnothing$ si ha $f(H) \neq \varnothing$. Per ogni $f(x), f(y) \in f(H)$ si ha $f(x)f(y) = f(xy) \in f(H)$ dato che $xy \in H$. Infine $\forall x \in H$ si ha $x^{-1} \in H$, quindi per ogni elemento $f(x) \in f(H)$ si ha $f(x)^{-1} = f(x^{-1}) \in f(H)$. Questo prova che $f(H) < G'$.
   Sia ora $K < G'$ allora $e' \in K$ e quindi $e \in f^{-1}(e') \subseteq f^{-1}(K)$. Per ogni $x, y \in f^{-1}(K)$ si ha che $f(x), f(y) \in K$ quindi, essendo K un sottogruppo e f un omomorfismo, $f(xy) = f(x)f(y) \in K$, quindi $xy \in f^{-1}(K)$. Infine se $x \in f^{-1}(K)$ si ha $x^{-1} \in f^{-1}(K)$ dato che $f(x^{-1}) = f(x)^{-1} \in K$.
3. Segue dal punto precedente applicato al caso $H = G$ e $K = \{e'\}$
4. Ovviamente se f è iniettivo in particolare si ha $\operatorname{Ker} f = f^{-1}(e') = \{e\}$.
   Viceversa sia $\operatorname{Ker} f = \{e\}$ e siano $x, y, \in G$ tali che $f(x) = f(y)$. Allora $e = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$, cioè $xy^{-1} \in \operatorname{Ker} f = \{e\}$, ossia $x = y$. ▲

Esempio 1.25.

1. La funzione $(\mathbb{R}, +) \longrightarrow (R^*, \cdot)$ definita da $x \mapsto e^x$ è un omomorfismo;
2. La funzione $\varphi_n : \mathbb{Z} \longrightarrow \mathbb{Z}$ definita da $\varphi_n(x) = nx$ è ovviamente un omomorfismo.
3. La proiezione $\pi_n : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ (definita da $\pi_n(a) = [a]_n$) è un omomorfismo per come abbiamo definito la somma tra classi di resto.

Proposizione 1.26. Sia $f : G \longrightarrow G'$ un omomorfismo. Allora

1. $\forall x \in G$ si ha $\operatorname{ord} f(x) \mid \operatorname{ord} x$ (con la convenzione che $n \mid +\infty$ e $+\infty \mid +\infty$).
2. f è iniettivo $\Leftrightarrow \operatorname{ord} f(x) = \operatorname{ord} x$, $\forall x \in G$.

DIMOSTRAZIONE.

1. Se $\operatorname{ord} x = +\infty$, non c'è niente da dimostrare.

   Sia quindi $d = \operatorname{ord} x$, quindi $x^d = e$ Applicando l'omomorfismo f otteniamo $f(x)^d = f(x^d) = f(e) = e'$, quindi $\operatorname{ord} f(x) \mid d$.

2. " $\Leftarrow$ " Se $f(x) = e'$ allora la condizione $\operatorname{ord} x = \operatorname{ord} f(x) = 1$ implica $x = e$.

   " $\Rightarrow$ " Supponiamo f iniettiva. Se $\operatorname{ord} f(x) = +\infty$ dal punto 1 segue che $\operatorname{ord} x = +\infty$; sia quindi $\operatorname{ord} f(x) = k$, allora $f(x^k) = (f(x))^k = e'$ e dall'iniettività di f segue che $x^k = e$, quindi $\operatorname{ord} x \mid k = \operatorname{ord} f(x)$. Usando anche il punto 1 otteniamo $\operatorname{ord} f(x) = \operatorname{ord} x$.

▲

Definizione 1.27. Un omomorfismo bigettivo si dice **isomorfismo**.
Due gruppi G e G' si dicono **isomorfi** se esiste un isomorfismo $f : G \longrightarrow G'$.

Osservazione 1.28. Due gruppi isomorfi sono sostanzialmente "uguali" dal punto di vista astratto. Infatti se $f : G \to G'$ è un isomorfismo allora, per il punto 2 della Proposizione precedente, conserva ordine degli elementi; inoltre l'applicazione che manda un sottogruppo H di G in $f(H)$ (che per la Proposizione[**?**] è un sottogruppo di G') dà una corrispondenza biunivoca tra i sottogruppi di G e i sottogruppi di G' .

Teorema 1.29. Sia G un gruppo ciclico.

1. Se G è infinito, allora $G \cong \mathbb{Z}$;
2. Se $|G| = n$, allora $G \cong \mathbb{Z}/n\mathbb{Z}$.

Dimostrazione.

Sia $G =< g >$. Se G è infinito, consideriamo la mappa

$$f : \mathbb{Z} \to G$$

$$k \mapsto g^k.$$

f è un omomorfismo perché $f(h+k) = g^{h+k} = g^h g^k = f(h)f(k)$.
f è iniettivo: infatti $\operatorname{Ker} f = \{k \mid g^k = e\}$ e essendo $G =< g >$ un gruppo infinito si ha che g ha ordine infinito, quindi $g^k = e$ se e solo se $k = 0$.
f è surgettivo perché $f(\mathbb{Z}) = \{g^k \mid k \in \mathbb{Z}\} =< g >= G$. Quindi f è un isomorfismo.

Sia ora $|G| = \operatorname{ord} g = n$; in questo caso definiamo la mappa

$$F : \mathbb{Z}/n\mathbb{Z} \to G$$
$$[a] \mapsto g^a$$

e mostriamo che F è un isomorfismo.
F è ben definita perché se $[a] = [a']$, cioè $a = a' + kn$ allora $g^a = g^{a'+kn} = g^{a'} g^{kn} = g^{a'} e = g^{a'}$.
F è un omomorfismo: la verifica banale è semplice ed è lasciata come esercizio.
F è surgettiva perché $\operatorname{Im} F = \{e, g, \ldots, g^{n-1}\} = G$.
F è iniettiva per motivi di cardinalità. ▲

Corollario 1.30. Sia $G =< g >$ un gruppo ciclico infinito. I suoi sottogruppi sono esattamente $< g^k >$ al variare di k in $\mathbb{N}$ e questa parametrizzazione li descrive tutti una e una sola volta.

Sia G un gruppo ciclico finito. G ha uno ed un solo sottogruppo di ordine d per ogni d tale che $d \mid |G|$.

Prodotto diretto di gruppi

Siano $(G_1, *_1)$ e $(G_2, *_2)$ due gruppi, consideriamo sull'insieme $G_1 \times G_2$ l'operazione definita da

$$(a, \alpha) * (b, \beta) := (a *_1 b, \alpha *_2 \beta)$$

$\forall (a, \alpha), (b, \beta) \in G_1 \times G_2$.

Proposizione 1.31. $(G_1 \times G_2, *)$ è un gruppo.

Dimostrazione.

Le verifiche sono banali.

- $G_1 \times G_2 \neq \varnothing$ perché G_1 e G_2 sono gruppi.
- L'operazione $*$ è ben definita perché se $(a, \alpha), (b, \beta) \in G_1 \times G_2$, allora $a *_1 b \in G_1$ e $\alpha *_2 \beta \in G_2$ e quindi $(a *_1 b, \alpha *_2 \beta) \in G_1 \times G_2$.
- $*$ è associativa (si verifica sfruttando l'associatività di $*_1$ e $*_2$).
- $(e_1, e_2) \in G_1 \times G_2$ è l'elemento neutro.
- $\forall (a, \alpha) \in G_1 \times G_2$ siano $a^{-1} \in G_1$ inverso di a e $\alpha^{-1} \in G_2$ inverso di α . Si verifica che (a^{-1}, α^{-1}) è l'inverso di (a, α) .

▲

Definizione 1.32. Il gruppo $(G_1 \times G_2, *)$ si dice **prodotto diretto** di $(G_1, *_1)$ e $(G_2, *_2)$.

Proposizione 1.33.

1. $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$.
   In particolare $G_1 \times G_2$ è abeliano $\Leftrightarrow$ G_1 e G_2 sono abeliani.
2. Siano G_1 e G_2 due gruppi. Per ogni $(x, y) \in G_1 \times G_2$
$$\operatorname{ord}(x, y) = [\operatorname{ord} x, \operatorname{ord} y].$$

DIMOSTRAZIONE.

1. La verifica è immediata.
2. Siano $m = \operatorname{ord} x$, $n = \operatorname{ord} y$ e $d = \operatorname{ord}(x, y)$.

   Allora $(x, y)^{[m,n]} = (x^{[m,n]}, y^{[m,n]}) = (e_1, e_2)$ in quanto $m = \operatorname{ord} x \mid [m, n]$ e $n = \operatorname{ord} y \mid [m, n]$. Ne segue che $d \mid [m, n]$.

   D'altra parte dalla relazione
$$(x^d, y^d) = (x, y)^d = (e_1, e_2)$$
   segue che $m \mid d$ e $n \mid d$ e quindi $[m, n] \mid d$.

▲

Teorema 1.34. (Teorema cinese del resto, III forma)
$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z} \Leftrightarrow (m, n) = 1.$$

DIMOSTRAZIONE.

" $\Leftarrow$ " $\operatorname{ord}([1]_m, [1]_n) = [m, n] = \frac{mn}{(m,n)} = mn$, quindi il gruppo $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ è ciclico, e quindi isomorfo a $\mathbb{Z}/mn\mathbb{Z}$.

" $\Rightarrow$ " Basta dimostrare che l'applicazione bigettiva definita dal Teorema cinese
$$\begin{array}{rccc} \varphi: & \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ & [a]_{mn} & \mapsto & ([a]_m, [a]_n) \end{array}$$
è un isomorfismo, cioè che $\varphi([a]_{mn} + [b]_{mn}) = \varphi([a]_{mn}) + \varphi([b]_{mn})$, e la verifica è banale. ▲

Classi laterali e insieme quoziente

Siano G un gruppo e H un suo sottogruppo.
Dati $x, y \in G$ diciamo che x è congruo a y modulo H (in simboli $x \sim_H y$) se $y^{-1}x \in H$.

Proposizione 1.35. $\sim_H$ è una relazione di equivalenza su G.

Dimostrazione.

- $\forall x \in G \ x \sim_H x$, infatti $x^{-1}x = e \in H$ perché $H < G$.
- se $x \sim_H y$ si ha $y^{-1}x \in H$ e, poiché H è un gruppo, anche $x^{-1}y = (y^{-1}x)^{-1} \in H$, cioè $y \sim_H x$.
- $\forall x, y, z \in G$ tali che $x \sim_H y$ e $y \sim_H z$ si ha $x \sim_H z$.
  Infatti dalle condizioni $y^{-1}x, z^{-1}y \in H$ segue che $z^{-1}x = (z^{-1}y)(y^{-1}x) \in H$.

▲

Definizione 1.36. Le classi di equivalenza di elementi di G rispetto alla relazione di equivalenza $\sim_H$ si chiamano **classi laterali sinistre**. Usiamo la notazione

$$[x]_H = \{y \in G \mid y \sim_H x\} = \{y \in G \mid x^{-1}y \in H\} = xH$$

Osservazione 1.37. Se $G = \mathbb{Z}$ e $H = n\mathbb{Z}$; la relazione di equivalenza modulo H non è altro che la congruenza modulo n (infatti in notazione additiva si ha $x \sim_H y$ se e solo se $x - y \in n\mathbb{Z}$). Di conseguenza le classi laterali sinistre di $n\mathbb{Z}$ in $\mathbb{Z}$ sono le classi di congruenza modulo n.

Le classi laterali sinistre danno una partizione di G. Detto X un insieme di rappresentanti delle classi laterali sinistre di H in G, si ha quindi

$$G = \overset{\circ}{\bigcup_{x \in X}} xH.$$

L'insieme $\{xH \mid x \in G\}$ si dice **l'insieme quoziente di G modulo H**.

Teorema 1.38. (Teorema di Lagrange.)
Sia G un gruppo finito e sia $H < G$. Allora $|H| \mid |G|$.

Dimostrazione.

Abbiamo la partizione

$$G = \overset{\circ}{\bigcup_{x \in X}} xH,$$

passando alle cardinalità si ha:

$$|G| = \sum_{x \in X} |xH|.$$

Poiché la funzione $H \longrightarrow xH$ definita da $h \mapsto xh$ è bigettiva, abbiamo $|H| = |xH| \forall x \in G$, quindi la formula sopra diventa $|G| = \#X \cdot |H|$ quindi $|H| \mid |G|$. ▲

Corollario 1.39. Sia G un gruppo finito. Allora

1. $\forall x \in G$, si ha $\operatorname{ord} x \mid |G|$.
2. $\forall x \in G$ si ha $x^{|G|} = e$.

Osservazione 1.40. Il teorema di Eulero è un caso particolare del corollario precedente

Corollario 1.41. Sia G un gruppo tale che $|G| = p$ con p primo. Allora $G \cong \mathbb{Z}/p\mathbb{Z}$.

Dimostrazione.

Poiché $|G| = p$ allora $\forall x \in G$ con $x \neq e$ si ha $\operatorname{ord} x = p$. Ne segue che $< x >= G$, in quanto un contenimento è ovvio e i due insiemi hanno la stessa cardinalità. Questo mostra che G è ciclico e avendo ordine p è isomorfo a $\mathbb{Z}/p\mathbb{Z}$. ▲

Definizione 1.42. $H < G$ definiamo **l'indice** di H in G

$$[G : H] = \#\text{classi laterali sx di } H \text{ in } G.$$

Se G è un gruppo finito si ha $[G : H] = |G|/|H|$.

Osservazione 1.43. In modo analogo a quanto fatto, si può definire un'altra relazione di equivalenza su G modulo H ponendo

$$x_H \sim y \quad \text{se} \quad xy^{-1} \in H$$

In questo modo le classi di equivalenza sono

$$[x] = Hx$$

e si chiamano classi laterali destre di H in G .

È semplice verificare che la funzione $xH \mapsto Hx$ defisce una corrispondenza biunivoca tra le classi laterali sinistre di H in G e le classi laterali destre, quindi queste sono nello stesso numero.

Nei gruppi abeliani (e non solo) si ha $Hx = xH \quad \forall x \in G$ ma questo non è vero in generale.

Esempio 1.44. $G = \mathcal{S}_3 = \{\mathrm{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ dove σ e τ sono definiti da

$$\sigma: \begin{array}{ccc} 1 & \mapsto & 2 \\ 2 & \mapsto & 3 \\ 3 & \mapsto & 1 \end{array} \qquad \tau: \begin{array}{ccc} 1 & \mapsto & 2 \\ 2 & \mapsto & 1 \\ 3 & \mapsto & 3 \end{array} \qquad \begin{array}{l} \mathrm{ord}\,\sigma = 3 \\ \mathrm{ord}\,\tau = 2 \end{array}$$

Prendiamo $H =< \tau >$. Le classi laterali sinistre di G modulo H sono: $H = \{\mathrm{id}, \tau\}$, $\sigma H = \{\sigma, \sigma\tau\}$, $\sigma^2 H = \{\sigma^2, \sigma^2\tau\}$, mentre quelle destre sono $H = \{\mathrm{id}, \tau\}$, $H\sigma = \{\sigma, \tau\sigma = \sigma^2\tau\}$, $H\sigma^2 = \{\sigma^2, \tau\sigma^2 = \sigma\tau\}$. In particolare $\sigma H \neq H\sigma$.

Sottogruppi Normali e Gruppo Quoziente

Definizione 1.45. Sia G un gruppo e $H < G$. Il sottogruppo H si dice **normale** in G (e si indica $H \lhd G$) se $\forall x \in G$ si ha $xH = Hx$.

Osservazione 1.46.

1. Se G è abeliano tutti i suoi sottogruppi sono normali.
2. La relazione $xH = Hx$ **non** vuol dire che $\forall h \in H$ vale $xh = hx$, ma è una relazione più debole.
3. $H \lhd G \Leftrightarrow \forall x \in G$, si ha $xHx^{-1} \subset H$.

   Infatti:

   " $\Rightarrow$ " è ovvio.

   " $\Leftarrow$ " La relazione vale $\forall x \in G$, quindi vale anche per x^{-1}, ossia $x^{-1}Hx \subset H$. Quindi $\forall x \in G xHx^{-1} = H$ o analogamente $\forall x \in G xH = Hx$.

Esempio 1.47.

1. G un gruppo, $\{e\}, Z(G), G \lhd G$.
2. $< \tau >$ non è sottogruppo normale di $\mathcal{S}_3$
3. Se $H < G$ e $[G : H] = 2$ allora $H \lhd G$.
   Infatti, se $\{H, xH\}$ è l'insieme delle classi laterali sx, allora $\{H, Hx\}$ è l'insieme delle classi laterali destre, e poiché

   $$G = H \overset{\circ}{\cup} xH = H \overset{\circ}{\cup} Hx,$$

   necessariamente $xH = Hx$, e si vede facilmente che $\forall g \in G$ vale $gH = Hg$.

Proposizione 1.48. Sia $f : G \longrightarrow G'$ un omomorfismo di gruppi. Allora:

1. $\mathrm{Ker}\, f \lhd G$;
2. $\forall x, y \in G$ $f(x) = f(y) \Leftrightarrow x$ e y sono nella stessa classe laterale modulo il nucleo.

Dimostrazione.

1. Siano $x \in G$ e $y \in \operatorname{Ker} f$ allora $f(xyx^{-1}) = f(x)f(y)f(x^{-1}) = f(x)e'f(x)^{-1} = e'$, quindi $x(\operatorname{Ker} f)x^{-1} \subset \operatorname{Ker} f$.
2. $f(x) = f(y) \Leftrightarrow f(y^{-1}x) = f(y)^{-1}f(x) = e'$
   $\Leftrightarrow y^{-1}x \in \operatorname{Ker} f \Leftrightarrow x \operatorname{Ker} f = y \operatorname{Ker} f$.

▲

Sia $N \lhd G$, poniamo

$$G/N := \{xN \mid x \in G\}$$

(è la stessa notazione usata per $\mathbb{Z}/n\mathbb{Z}$!!)

Possiamo definire sull'insieme G/N una struttura di gruppo "indotta da quella di G ", ponendo

$$xN \cdot yN := xyN.$$

Poiché la definizione è data in termini di rappresentanti, occorre verificare che sia ben definita, cioè che se $xN = x'N$ e $yN = y'N$ allora $xyN = x'y'N$.

Ora se $x'^{-1}x \in N$ e $y'^{-1}y \in N$ si ha

$$(x'y')^{-1}xy = y'^{-1}x'^{-1}xy = y'^{-1}ny \overset{\substack{N \lhd G \\ \downarrow}}{=} y'^{-1}yn' = n'' \in N$$

con $n, n', n'' \in N$, quindi $xyN = x'y'N$.

Osservazione 1.49. Se N non fosse un sottogruppo normale di G l'operazione definita non sarebbe in generale ben posta.

Infatti se $G = \mathcal{S}_3$ e $H =< \tau >$ si ha
$\sigma H = \sigma\tau H$, $\sigma^2 H = \sigma^2\tau H$, $\sigma^3 = \mathrm{id}$, $\sigma\tau\sigma^2\tau = \sigma^2$ e $H \neq \sigma^2 H$.

Proposizione 1.50.
1. G/N con l'operazione definita è un gruppo (si chiama **gruppo quoziente**).
2. La proiezione $\pi_N : G \longrightarrow G/N$ definita da $\pi_N(x) = xN$ è un omomorfismo surgettivo di gruppi con nucleo N .

Dimostrazione.

1. Si verifica facilmente.
2. Siano $x, y \in G$ allora $\pi_N(xy) = xyN = xN \cdot yN = \pi_N(x) \cdot \pi_N(y)$ per come è definito il prodotto tra classi.

   L'omomorfismo π_N è surgettivo per definizione di gruppo quoziente. Inoltre $\operatorname{Ker} \pi_N = \{x \in g \mid xN = N\} = N$. ∎

▲

Osservazione 1.51. Con la notazione introdotta possiamo dire che $\mathbb{Z}/n\mathbb{Z}$ è il gruppo quoziente di $\mathbb{Z}$ rispetto a $n\mathbb{Z}$. Infatti l'operazione tra le classi era stata definita ponendo $(a+n\mathbb{Z})+(b+n\mathbb{Z})=(a+b)+n\mathbb{Z}$.

Corollario 1.52. I sottogruppi normali di un gruppo G sono tutti e soli i nuclei degli omomorfismi.

Dimostrazione.

Abbiamo già visto nella Proposizione 1.48 che i nuclei degli omomorfismi sono sottogruppi normali di G.

Viceversa se $N \lhd G$ allora $N = \operatorname{Ker} \pi_N$. ▲

Teorema 1.53. (**I Teorema di omorfismo di gruppi**)
Sia $f : G \longrightarrow G'$ un omomorfismo di gruppi e sia $N \lhd G$ tale che $N \subseteq \operatorname{Ker} f$. Allora esiste uno e un solo omomorfismo $\varphi : G/N \longrightarrow G'$ tale che il diagramma seguente sia commutativo

$$\begin{array}{ccc} & G & \xrightarrow{f} & G' \\ \pi_N & \downarrow & \nearrow_{\varphi} & \\ & G/N & & \end{array}$$

Per tale omomorfismo si ha $\operatorname{Im}\varphi = \operatorname{Im} f$, e $\operatorname{Ker}\varphi = \operatorname{Ker} f/N$.

Dimostrazione.

Se φ esiste allora è sicuramente unica poiché dalla relazione $\varphi \circ \pi_N = f$ si ha $\varphi(\pi_N(x)) = f(x)$ per ogni $x \in G$, e quindi $\varphi(xN) = f(x)$.

Occorre vedere che φ può essere definita in questo modo e che risulta un omomorfismo.

Per prima cosa osserviamo che la φ che fa commutare il diagramma è una funzione ben definita, cioè che il valore di $\varphi(xN) = f(x)$ non dipende dal rappresentante scelto per la classe laterale. Sia quindi $xN = yN$, allora vale anche $x \operatorname{Ker} f = y \operatorname{Ker} f$ e quindi, per la Proposizione 1.48, $f(x) = f(y)$ e la definizione della φ non dipende dal rappresentante scelto per la classe xN.

Osserviamo anche che φ è un omomofismo, infatti: $\varphi(xN \cdot yN) = \varphi(xyN) = f(xy) = f(x)f(y) = \varphi(xN)\varphi(yN)$.

Inoltre $\varphi(G/N) = \varphi(\pi_N(G)) = f(G)$, cioè $\operatorname{Im}\varphi = \operatorname{Im} f$.

Calcoliamo il nucleo: $xN \in \operatorname{Ker}\varphi$ se e solo se $\varphi(xN) = f(x) = e'$ cioè se e solo se $x \in \operatorname{Ker} f$. Quindi si ha che $\operatorname{Ker} f = \{xN \mid x \in \operatorname{Ker} f\} = N/\operatorname{Ker} f$. ▲

Corollario 1.54. Con le notazioni del teorema, se f è surgettivo e $N = Ker f$ si ha che $\varphi : G/N \to G'$ è un isomorfismo.

Corollario 1.55. (II teorema di omomorfismo)
Siano $H, K \lhd G$ e sia $H \subseteq K$. Allora

$$\frac{G/H}{K/H} \cong G/K$$

.

Corollario 1.56. (III teorema di omomorfismo)
Siano $H, K \lhd G$. Allora

$$\frac{H}{K \cap H} \cong HK/K$$

.

Corrispondenza tra sottogruppi.

Sia $N \lhd G$ e sia $\pi_N : G \to G/N$ la proiezione.

Grazie alla Proposizione 1.24 si ha che per ogni $H < G$, la sua immagine $\pi_N(H)$ è un sottogruppo di G' e, viceversa, per ogni $\mathcal{H} < G/N$, si ha $\pi_N^{-1}(\mathcal{H}) < G$ e vale $N = \pi_N^{-1}(eN) \subseteq \pi_N^{-1}(\mathcal{H})$.

Poniamo $X = \{H < G \,|\, N \subseteq H\}$ e $Y = \{\mathcal{H} < G/N\}$; vale il seguente teorema:

Teorema 1.57. La mappa π_N induce una corrispondenza biunivoca tra i sottogruppi di G che contengono N e i sottogruppi di G/N . Questa corrispondenza conserva i sottogruppi normali e l'indice di sottogruppo.

Dimostrazione.

Siano $\alpha : X \to Y$ e $\beta : Y \to X$ le mappe definite da $\alpha(H) = \pi_N(H)$ e $\beta(\mathcal{H}) = \pi_N^{-1}(\mathcal{H})$ (cioè le mappe indotte rispettivamente da π_N e da π_N^{-1}). Per quanto osservato sopra queste mappe sono ben definite; è semplice vedere anche che $\alpha(H) = \pi_N(H) = H/N$ in quanto $N \subseteq H$. Mostriamo che sono una l'inversa dell'altra, e quindi bigettive.

Dalla surgrettività di π_N si ottiene che $\alpha(\beta(\mathcal{H})) = \pi_N(\pi_N^{-1}(\mathcal{H})) = \mathcal{H}$. D'altra parte $\beta(\alpha(H)) = \pi_N^{-1}(\pi_N(H)) = \pi_N^{-1}(H/N) = HN = H$ dove l'ultima uguaglianza segue dal fatto che $N \subseteq H$.

Rimane da mostrare che α fa corrispondere sottogruppi normali a sottogruppi normali (questa verifica è semplice, ma attenzione è fondamentale usare la surgettività di π_N) e che conserva l'indice di sottogruppo, cioè che $[G : H] = [G/N : \pi_N(H)]$ per ogni $H \in X$. Poichè $\pi_N(H) = H/N$, occorre mostrare che $xH = yH$ se e solo se $xNH/N = yNH/N$ cioè se $xH/N = yN/N$. questo è vero perché queste condizioni sono soddisfatte se e solo se $y^{-1}x \in H$.

▲