Alma Mater Studiorum · Università di Bologna

CORSO DI LAUREA IN MATEMATICA

RETICOLI DI SOTTOGRUPPI

Presentata da:
Maria Narciso

Relatore:
Prof.ssa Marta Morigi

Sessione
2019/2020

Introduzione

I reticoli di sottogruppi sono una particolare struttura i cui elementi sono sottogruppi di un gruppo G. In questo elaborato si descriveranno queste strutture che hanno una importanza particolare in quanto è stato dimostrato da Whitman che ogni reticolo è isomorfo a un sottoreticolo di un reticolo di sottogruppi di un certo gruppo.
Viene spontaneo chiedersi quali informazioni possiamo dedurre su un gruppo G a partire dal reticolo dei suoi sottogruppi. Certamente non è possibile individuare la sua classe di isomorfismo, perché esistono, ad esempio, gruppi ciclici non isomorfi, che però hanno lo stesso reticolo dei sottogruppi. D'altra parte, il reticolo dei sottogruppi di un gruppo fornisce molte informazioni sul gruppo, e il teorema di Ore costituisce un importante risultato in questa direzione.
Nel primo capitolo si descrivono aspetti generali della teoria dei reticoli. Nel secondo capitolo si studiano alcuni reticoli di sottogruppi, in particolare il reticolo dei sottogruppi di composizione. In questo ambito, sono di importanza fondamentale i sottogruppi subnormali e il lemma di Zassenhaus. Nel terzo capitolo si dimostra il teorema di Ore, che afferma che il reticolo dei sottogruppi di un gruppo è distributivo se e solo se il gruppo è localmente ciclico, cioè ogni suo sottogruppo finitamente generato è ci-

clico.
Grazie a questo teorema è possibile dare qualche caratterizzazione dei reticoli dei gruppi ciclici. Inoltre si studiano alcuni reticoli di sottogruppi che sono modulari, ad esempio il reticolo dei sottogruppi normali di un gruppo.

Indice

Capitolo 1

Prime definizioni

1.1 Insieme parzialmente ordinato e reticolo

I primi due concetti di cui abbiamo bisogno sono la definizione di poset (insieme parzialmente ordinato) e di reticolo, che vedremo poi essere un poset dotato di particolari caratteristiche.

Definizione 1.1.1. Un insieme parzialmente ordinato (o poset) è un insieme P dotato di una relazione $\leq$ tale che per ogni $x, y, z \in P$ sono soddisfatte le seguenti condizioni:

$$x \leq x \quad \text{(riflessività)} \tag{1.1}$$

$$\text{Se} \quad x \leq y \quad \text{e} \quad y \leq x \quad \text{allora} \quad x = y \quad \text{(antisimmetria)} \tag{1.2}$$

$$\text{Se} \quad x \leq y \quad \text{e} \quad y \leq z \quad \text{allora} \quad x \leq z \quad \text{(transitività)} \tag{1.3}$$

Definizione 1.1.2. Un elemento x di un poset è detto *minorante* per un sottoinsieme S di P se $x \leq s$ per ogni $s \in S$. L'elemento x è detto *estremo*

inferiore per S se x è un minorante di S e $y \leq x$ per ogni minorante y di S. Esso è un *minimo* se $x \in S$. L'elemento x si dice invece *maggiorante* per un sottoinsieme S di P se $s \leq x$ per ogni $s \in S$. Infine, x è detto *estremo superiore* per S se x è maggiorante di S e $x \leq y$ per ogni maggiorante y di S. Esso è un *massimo* se $x \in S$.
Per la proprietà (1.2), se l'estremo inferiore esiste, è unico, e lo indichiamo con inf S o con $\bigwedge S$. La stessa cosa si applica alle definizioni di maggiorante e di estremo superiore, denotato invece con sup S o $\bigvee S$.

Osservazione 1.1.3. Può succedere che S abbia vari minoranti e non un minimo. Analogamente, possiamo notare le stesse cose riguardo maggiorante e massimo. Denotiamo con O e I rispettivamente il minimo e il massimo di S.

Ora siamo pronti per dare la definizione di reticolo.

Definizione 1.1.4. Un *reticolo* è un insieme parzialmente ordinato in cui, presi due elementi qualsiasi, essi hanno un estremo superiore e uno inferiore. Un poset P in cui ogni sottoinsieme S ha un estremo inferiore e uno superiore è detto *reticolo completo.*

Teorema 1.1.5. *Sia* $(L, \leq)$ *un reticolo con le operazioni* $\wedge$ *e* $\vee$ *definite da:*

$$x \wedge y = \inf \{x, y\} \quad e \quad x \vee y = \sup \{x, y\} \tag{1.4}$$

Allora per ogni $x, y, z \in L$ valgono le seguenti proprietà:

$$x \wedge y = y \wedge x \quad e \quad x \vee y = y \vee x \qquad \textit{(commutatività)} \tag{1.5}$$

$$(x \wedge y) \wedge z = x \wedge (y \wedge z) \quad e \quad (x \vee y) \vee z = x \vee (y \vee z) \quad \textit{(associatività)} \tag{1.6}$$

$$x \wedge (x \vee y) = x \quad e \quad x \vee (x \wedge y) = x \qquad \textit{(assorbimento)} \tag{1.7}$$

Inoltre, abbiamo che $x \leq y$ se e solo se $x = x \wedge y$.

Dimostrazione. Osserviamo subito che le operazioni definite in (1.4) sono commutative, dunque vale la (1.5).
Inoltre $x \wedge (y \wedge z)$ e $(x \wedge y) \wedge z$ sono entrambi il minimo dell'insieme $\{x, y, z\}$ e quindi vale anche (1.6). Allo stesso modo, si verificano entrambe le equazioni per $\vee$.
Infine, $x \leq y$ se e solo se $x = \inf\{x, y\} = x \wedge y$ e poiché $x \leq y \wedge x$ e $x \wedge y \leq x$, allora vale anche la (1.7). □

Il prossimo teorema è l'inverso del precedente

Teorema 1.1.6. *Sia L un insieme dotato di operazioni binarie $\wedge$ e $\vee$ che soddisfano (1.5) e (1.7), e della relazione $\leq$ su L tale che*

$$x \leq y \quad \textit{se e solo se} \quad x = x \wedge y \tag{1.8}$$

Allora L è un reticolo e vale (1.4).

Dimostrazione. Siano $x, y, z \in L$. Vogliamo mostrare che $x \wedge y = x$ è equivalente a dire che $y \vee x = y$.
Infatti $y \vee x = y \vee (y \wedge x) = y$ e inoltre $x \wedge y = x \wedge (y \vee x) = x$, e allora, grazie alla proprietà (1.8), otteniamo che

$$x \leq y \quad \text{se e solo se } y = y \vee x \tag{1.9}$$

Infine, mostriamo che $(L, \leq)$ è un poset.
La proprietà di assorbimento ci permette di dire che $x \wedge x = x \wedge (x \vee (x \wedge x)) = x$, dunque, per (1.8), $x \leq x$, quindi vale la (1.1).
Se $x \leq y$ e $y \leq x$ allora $x = x \wedge y = y \wedge x = y$ e dunque vale la (1.2).
Infine, se $x \leq y$ e $y \leq z$, allora $x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x$, quindi $x \leq z$ e vale la proprietà (1.3).
Dunque abbiamo dimostrato che L è un poset. Ora mostriamo che le operazioni in (1.4) sono ben definite.
Sappiamo già che

$$(x \wedge y) \wedge x = x \wedge (x \wedge y) = (x \wedge x) \wedge y = x \wedge y$$

allora $x \wedge y \leq x$ e analogamente si ha che $x \wedge y \leq y$.
Inoltre, se z è un minorante di $\{x, y\}$ allora $z \wedge x = z$ e $z \wedge y = z$, quindi

$$z \wedge (x \wedge y) = (z \wedge x) \wedge y = z \wedge y = z$$

e $z \leq x \wedge y$. Questo mostra che $x \wedge y = \inf \{x, y\}$. Usando $\vee$ al posto di $\wedge$ e usando la proprietà (1.9) al posto della (1.8) otteniamo che $x \vee y = \sup \{x, y\}$. In particolare, $(L, \leq)$ è un reticolo. □

1.2 Minimi, massimi, catene e anticatene

Definizione 1.2.1. Per due elementi x, y di un poset P, scriviamo $x < y$ se $x \leq y$ e $x \neq y$. Se $x < y$ e non esiste un elemento z tale che $x < z < y$, allora diciamo che x è coperto da y o che y copre x.

Definizione 1.2.2. Un elemento di P che copre O è detto *atomo*. Un elemento di P che è coperto da 1 è detto *antiatomo*. Se L è un reticolo completo, allora inf L è il suo minimo, sup L è il massimo.
Due elementi x e y di un poset P sono detti $confrontabili$ se $x \leq y$ oppure $y \leq x$.

Definizione 1.2.3. Un sottoinsieme S di P è una *catena* se, presi due elementi qualsiasi di S, essi sono confrontabili. S è una *anticatena* se nessuno dei suoi elementi è confrontabile con gli altri. La lunghezza di una catena finita S è $|S| - 1$.

Definizione 1.2.4. Un poset P è detto di lunghezza n, con $n \in \mathbb{N}$, se esiste una catena di lunghezza n contenuta dentro P tale che tutte le altre catene di P abbiano lunghezza al più n. Un poset P ha lunghezza finita se la sua lunghezza è al più n, con $n \in \mathbb{N}$.
Allo stesso modo, un poset P è di ampiezza n se esiste una anticatena S con n elementi tale che tutte le altre anticatene hanno al più n elementi.

Definizione 1.2.5. Si dice che un poset P soddisfa la condizione di massimalità (o condizione della catena ascendente) se ciascuno dei suoi sottoinsiemi non vuoti contiene un elemento massimale.
Equivalentemente, possiamo dire che P soddisfa la condizione di massimalità se e solo se non contiene successioni infinite di elementi $x_1, x_2, ...$ tali che $x_1 < x_2 < x_3....$ Analogamente, possiamo dare la definizione di condizione di minimalità o della catena discendente.

Definizione 1.2.6. Un sottoinsieme di un reticolo è detto *sottoreticolo* se è chiuso rispetto alle operazioni $\wedge$ e $\vee$ definite in 1.1.5. Ovviamente, un sottoreticolo è un reticolo con le operazioni indotte.

Esempi di sottoreticoli di un reticolo L sono, per $x, y \in L$, gli insiemi del tipo $S = \{x, y, x \wedge y, x \vee y\}$, oppure, se $x \leq y$, gli intervalli del tipo $[x, y] = \{z \in L \mid x \leq z \leq y\}$

1.3 Isomorfismi tra reticoli e diagramma di Hasse

Definizione 1.3.1. Siano $L, \tilde{L}$ due reticoli. Una mappa σ: $L \to \tilde{L}$ è detto *omomorfismo* se, per ogni $x, y \in L$

$$(x \wedge y)^\sigma = x^\sigma \wedge y^\sigma \quad \text{e} \quad (x \vee y)^\sigma = x^\sigma \vee y^\sigma \tag{1.10}$$

Definizione 1.3.2. Un omomorfismo è detto *isomorfismo* se è biiettivo, mentre è detto *automorfismo* se è un isomorfismo di un reticolo in se stesso. Scriviamo quindi che $L \simeq \tilde{L}$ se L e $\tilde{L}$ sono isomorfi.

Teorema 1.3.3. *Sia σ una mappa biiettiva $\sigma : L \to \tilde{L}$. Allora, le seguenti affermazioni sono equivalenti:*

1. *Per ogni $x, y \in L$, $x \leq y$ se e solo se $x^\sigma \leq y^\sigma$*
2. *$(x \wedge y)^\sigma = x^\sigma \wedge y^\sigma$ per ogni $x, y \in L$*
3. *$(x \vee y)^\sigma = x^\sigma \vee y^\sigma$ per ogni $x, y \in L$*

Inoltre, se σ soddisfa (1.) e se S sottoinsieme di L tale che $\bigwedge S$ esiste, allora anche $\bigwedge S^\sigma$ esiste e si ha che $(\bigwedge S)^\sigma = \bigwedge S^\sigma$.
Analogamente, valgono le stesse relazioni per $\bigvee S$.

Dimostrazione. Siano $x, y \in L$. Sappiamo già da 1.1.5 che $x \leq y$ se e solo se $x \wedge y = x$ oppure $x \vee y = y$. Quindi 2) $\Rightarrow$ 1) e di conseguenza, anche 3) $\Rightarrow$ 1).
Viceversa, se σ soddisfa 1) e se S è un sottoinsieme di L tale che $z = \bigwedge S$ esiste, allora z^σ è un minorante di S. Poiché z è il minimo di S, se w è un altro minorante di S, sappiamo che $w \leq z$ e dunque $w^\sigma \leq z^\sigma$. Questo mostra che z^σ è il minimo di S^σ e che $(\bigwedge S)^\sigma = \bigwedge S^\sigma$, dunque abbiamo ottenuto anche che 1) $\Rightarrow$ 2). Analogamente si verifica che 1) $\Rightarrow$ 3). $\square$

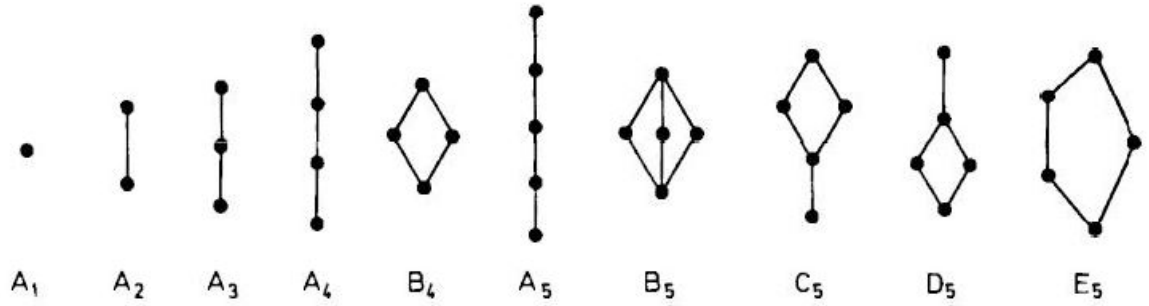
Osservazione 1.3.4. Per mostrare che una mappa biiettiva tra due reticoli è un isomorfismo, è sufficiente far vedere che una delle due relazioni del

teorema precedente (la seconda e la terza) è vera o che la mappa preserva la relazione d'ordine di cui sono dotati i reticoli.

Vediamo un modo per rappresentare i reticoli.

Definizione 1.3.5. Ogni P poset finito, in particolare ogni reticolo finito, può essere rappresentato con un diagramma. Esso rappresenta ogni elemento di P con un punto del piano in modo che il punto P_y associato a un elemento y si trovi sopra al punto associato a x per ogni $x < y$. Allora, ogni qualvolta y copre x, colleghiamo i punti P_x e P_y con un segmento di retta. Chiamiamo la figura risultante *diagramma di Hasse* di P.

Osservazione 1.3.6. Si può facilmente vedere che è possibile costruire il diagramma di Hasse con un processo induttivo. Sia z l'elemento massimale del poset finito P, allora, posto $S = P\backslash\{z\}$, questo è un poset di lunghezza minore e allora, per induzione, ha un diagramma.
Dunque, scegliamo un punto P_z sopra i punti del diagramma di S e lo colleghiamo con tutti i punti P_x associati agli elementi x che sono coperti da z. Qui di seguito riportiamo alcuni esempi.



1.4 Prodotti diretti

Definizione 1.4.1. Sia $(L_\lambda)_{\lambda\in\Lambda}$. una famiglia di reticoli. Il prodotto diretto

$$L = \prod_{\lambda\in\Lambda} L_\lambda$$

è il reticolo il cui insieme sottostante è il prodotto cartesiano degli insiemi L_λ, che è a sua volta l'insieme di tutte le funzioni f definite su Λ tali che $f(\lambda) \in L_\lambda$ per tutti i $\lambda \in \Lambda$ e il cui ordine parziale è definito dalla relazione $f \leq g$ se e solo se $f(\lambda) \leq g(\lambda)$ per ogni $\lambda \in \Lambda$.
Osserviamo che $f \wedge g$ e $f \vee g$ sono le funzioni che mandano ogni λ in $f(\lambda) \wedge g(\lambda)$ e in $f(\lambda) \vee g(\lambda)$ rispettivamente. Quindi L è un reticolo le cui operazioni sono definite componente per componente. Questo significa che L è un reticolo se e solo se lo è ogni L_λ.
Inoltre, se Λ è finito di cardinalità n, allora $L = L_1 \times ... \times L_n = \{(x_1, ..., x_n)$; $x_i \in L_i\}$ e si ha che $(x_1, ..., x_n) \leq (y_1, ..., y_n)$ se e solo se $x_i \leq y_i$ per ogni $i = 1, ..., n$.

Vediamo alcune proprietà del prodotto diretto di reticoli

Teorema 1.4.2. *Sia L definito come sopra. Supponiamo che L contenga un minimo O e un massimo I. Se $\lambda \in \Lambda$, allora $O(\lambda)$ è il minimo di L_λ e $I(\lambda)$ è il massimo di L_λ. Definiamo quindi $f_\lambda \in L$ tale che $f_\lambda(\mu) = O(\mu)$ per $\lambda \neq \mu$ e $f_\lambda(\lambda) = I(\lambda)$. Allora sono vere le seguenti affermazioni:*

$$\bigvee_{\nu\in\Lambda} f_\nu = I \quad e \quad (\bigvee_{\nu\in\Lambda\setminus\{\lambda\}} f_\nu) \wedge f_\lambda = O \tag{1.11}$$

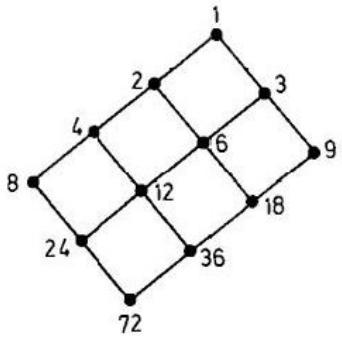
$$[f_\lambda, O] \simeq L_\lambda \tag{1.12}$$

$$[x \wedge y, O] \simeq [x, O] \times [y, O] \text{ se } x, y \in [f_\lambda, O] \text{ e } \lambda \neq \mu \in \Lambda \tag{1.13}$$

Dimostrazione. Per $z \in L_\lambda$, l'assioma della scelta implica che esiste una funzione $f \in L$ tale che $f(\lambda) = z$. Per $O \leq f \leq I$ segue che $O(\lambda) \leq f(\lambda) \leq I(\lambda)$. Questo mostra che $O(\lambda)$ è il minimo di L_λ e che $I(\lambda)$ è il massimo di L_λ. Poiché sup e inf sono definiti componente per componente, abbiamo che (1.11) è vera.
Ora, definiamo la mappa $\sigma : L_\lambda \to [f_\lambda, O]$ tale che $z^\sigma(\nu) = O(\nu)$ per $\lambda \neq \nu \in \Lambda$ e $z^\sigma(\lambda) = z$. Per come lo abbiamo definito, σ è un isomorfismo, quindi anche (1.12) è vera.
Infine, sia $\tau : [x, O] \times [y, O] \to [x \wedge y, O]$ la funzione che manda la coppia (u, v) in w tali che $w(\lambda) = u(\lambda)$, $w(\mu) = v(\mu)$ e $w(\nu) = O(\nu)$ per $\nu \in \Lambda$ con $\lambda \neq \nu \neq \mu$. Anche τ è un isomorfismo e quindi abbiamo mostrato anche la (1.13). □

Ora, costruiamo un reticolo fondamentale. Per $a, b \in \mathbb{N}$ (escludendo lo zero dai naturali) diciamo che $a \leq b$ se b divide a. Naturalmente, $\leq$ è una relazione di ordine parziale su $\mathbb{N}$, per cui abbiamo che sup $\{a, b\}$ è

il massimo comun divisore tra a e b e che inf $\{a, b\}$ è il minimo comune multiplo tra a e b.
Dunque $(\mathbb{N}, \leq)$ è un reticolo e lo tenotiamo con T_∞ e scriviamo per ogni $n \in \mathbb{N}$ il reticolo T_n per l'intervallo $[1, n]$ in T_∞ e otteniamo che T_n è il reticolo di tutti i divisori di n. Vediamo l'esempio per $n = 72$



Proposizione 1.4.3. *Sia $n = p_1^{k_1} \cdot ... \cdot p_r^{k_r}$ con p_i primi distinti. Allora si ha che $T_n \simeq T_{p_1^{k_1}} \times ... \times T_{p_r^{k_r}}$.*

Dimostrazione. Osserviamo che, per come è stato definito, $T_n = \{m \ ; \ m|n\}$, mentre $T_{p_1^{k_1}} \times ... \times T_{p_r^{k_r}} = \{(p_1^{i_1}, ..., p_r^{i_r}) \mid 0 \leq i_j \leq k_j\}$. Ora, sia $m \in T_n$, allora $m = p_1^{\beta_1} \cdot ... \cdot p_r^{\beta_r}$ con $\beta_j \leq k_j$ per ogni $j = 1, ..., r$, dunque costruiamo

$$\phi : T_n \to T_{p_1^{k_1}} \times ... \times T_{p_r^{k_r}}$$

tale che $\phi(m) = \phi(p_1^{\beta_1} \cdot ... \cdot p_r^{\beta_r}) = (p_1^{\beta_1}, ..., p_r^{\beta_r})$. Si verifica facilmente che ϕ è l'isomorfismo richiesto. □

Capitolo 2

Reticoli di sottogruppi

2.1 Preliminari di teoria dei gruppi

Poiché dovremo caratterizzare i reticoli di sottogruppi, richiamiamo alcune definizioni utili.

Definizione 2.1.1. Siano H, K sottogruppi di G. Si dice che H è *normalizzato* da K se, per ogni $h \in H$ e per ogni $k \in K$, si ha che $h^{-1}kh \in K$.

Teorema 2.1.2. *Sia* $HK = \{hk$ *tale che* $h \in H$ *e* $k \in K\}$*, se* H *è normalizzato da* K*, esso è un sottogruppo e in particolare abbiamo che* $HK = KH$*.*

Dimostrazione. Sia $kh \in KH$. Sappiamo che $h^{-1}kh = \bar{k} \in K$, allora abbiamo che $kh = h\bar{k}$ e dunque $KH \subseteq HK$.
Viceversa, sia $hk \in HK$, allo stesso modo abbiamo che $hkh^{-1} = \bar{k} \in K$ e quindi $hk = \bar{k}H \in KH$, e dunque $HK \subseteq KH$. Abbiamo la doppia inclusione e quindi $HK = KH$.

Utilizzando questo fatto, possiamo mostrare che HK è un sottogruppo. Infatti siano h_1k_1 e h_2k_2 due elementi di HK, allora $h_1k_1h_2k_2 = h_1\bar{h}\bar{k}k_2$ perché $HK = KH$. Dunque otteniamo che $h_1\bar{h} \in$ H e $\bar{k}k_1 \in$ K e dunque

$$h_1k_1h_2k_2 \in HK = KH$$

Per l'inverso, invece, notiamo che $(hk)^{-1} = k^{-1}h^{-1} \in HK = KH$. Dall'inverso, posso ottenere l'elemento neutro e dunque ho mostrato che HK è un sottogruppo. □

Qui di seguito, daremo la definizione di omomorfismo per quanto riguarda i gruppi. La definizione si rivelerà analoga a quella per i reticoli.

Definizione 2.1.3. Dati due gruppi $(G, \star)$ e $(G', \diamond)$, un *omomorfismo* è una funzione $f : G \to G'$ tale che, per ogni $g_1, g_2 \in G$, si ha che

$$f(g_1 \star g_2) = f(g_1) \diamond f(g_2)$$

Un omomorfismo f è detto *isomorfismo* se f è biiettiva.

Definizione 2.1.4. Il *nucleo* di un omomorfismo f è definito come
Ker $f = \{g \in G \mid f(g) = e_{G'}\}$

Ora siamo pronti per enunciare i tre teoremi di isomorfismo per i gruppi. Ricordiamo il primo teorema di isomorfismo.

Teorema 2.1.5 (Primo teorema di isomorfismo)**.** *Sia $f : G \to H$ un omomorfismo e sia $K = Ker\, f$. Allora K è un sottogruppo normale di G e inoltre $G/K \cong Imf$.*

Teorema 2.1.6 (Secondo teorema di isomorfismo)**.** *Siano N e T due sottogruppi di un gruppo G con N sottogruppo normale di G. Allora $N \cap T$ è normale in T e*

$$T/(N \cap T) \simeq NT/N$$

Dimostrazione. Sia $v : G \to G/N$ la funzione che manda g in gN per ogni $g \in G$. Sia $v' = v|_T$ la restrizione di v a T. Si ha che v' è banalmente un omomorfismo, e se mostriamo che il suo nucleo è effettivamente $N \cap T$, possiamo concludere grazie al primo teorema di omomorfismo. In effetti,

$$\text{Ker } v' = \{t \in T \mid v'(Nt) = e\} = \{t \in T \,;\, t \in N\} = N \cap T$$

L'immagine di v' è NT/T per come l'abbiamo definita e dunque possiamo concludere. □

Teorema 2.1.7 (Terzo teorema di isomorfismo)**.** *Siano $K \leq H \leq G$ con H e K sottogruppi normali di G. Allora H/K è un sottogruppo normale di G/K e si ha che*

$$(G/K)(H/K) \simeq G/H$$

Dimostrazione. Anche qui la nostra intenzione è quella di applicare il primo teorema di isomorfismo. Definiamo quindi $\psi : G/K \to G/H$ e

ancora una volta facciamo vedere che Ker $\psi = H/K$. Questo è vero perché Ker $\psi = \{Ka \in G/K; \psi(Ka) = e\} = \{Ka \in G; Ka \in H\} = \{Ka \in G; a \in H/K\} = H/K$, allora Ker $\psi = H/K$ e quindi abbiamo concluso. □

2.2 Reticoli di sottogruppi

Qui di seguito diamo le definizioni di reticolo di sottogruppi e di serie di composizione e studiamo alcune proprietà dei reticoli di serie di composizione.

Definizione 2.2.1. Sia G un gruppo. Si definisce il *reticolo dei sottogruppi*, indicato con $L(G)$, l'insieme di tutti i sottogruppi di G, ordinato con la relazione di inclusione in cui, presi $A, B \leq G$, si ha che $\langle A, B\rangle = A \vee B$, che è il sottogruppo generato da A e da B, e che $A \cap B = A \wedge B$.
Osserviamo che $L(G)$ è un reticolo completo, in quanto ha un minimo, che è il sottogruppo identico, e un massimo, che è G.

Qui di seguito, diamo un risultato che si rivelerà fondamentale per dimostrare i prossimi teoremi.

Proposizione 2.2.2. *Siano H, K due sottogruppi con H normalizzato da K. Allora si ha che $HK = H \vee K = KH$.*

Dimostrazione. Dalla definizione sappiamo che $H \vee K = \langle H, K \rangle$. Ora, l'inclusione $HK \subseteq \langle H, K \rangle$ è ovvia. Per l'inclusione inversa, osserviamo che $\langle H, K \rangle$ è il più piccolo sottogruppo che contiene H e K. Ora mostriamo che $H, K \in HK$ e questo è vero in quanto ogni $h \in H$ si può scrivere come $h = he_k \in HK$ e ogni $k \in K$ lo posso scrivere come $k = e_h k \in HK$. Ora, poiché H è normalizzato da K, abbiamo per il Teorema 2.1.2 che HK è un sottogruppo e in particolare $HK = KH$. Questo vuol dire che $HK \supseteq \langle H, K \rangle$ e quindi abbiamo concluso. □

Un esempio di reticolo di sottogruppi è il reticolo dei sottogruppi normali di un gruppo G definito come $\mathfrak{R}(G) = \{N; N \trianglelefteq G\}$.

Ora definiamo i sottoreticoli inferiori di un reticolo L e diamo prova di alcune loro proprietà.

Definizione 2.2.3. Sia L un reticolo e sia M un sottoinsieme di L che è un reticolo rispetto all'ordine parziale indotto e siano $\wedge$ e $\cap$ rispettivamente le due operazioni di L e M. Allora, per $x, y \in M$, $x \cap y$ è un minorante di $\{x, y\}$ in L e $x \cap y \leq x \wedge y$. Chiamiamo M un *sottoreticolo inferiore* se $x \cap y = x \wedge y$ per ogni $x, y \in M$.
M è inoltre un *sottoreticolo inferiore completo* se M e L sono reticoli completi e se per ogni sottoinsieme S di M l'estremo inferiore di S in M e quello di S in L coincidono.

Chiaramente, non è detto che M sia un sottoreticolo di L, infatti il reticolo dei sottogruppi di un gruppo G come sottoinsieme del reticolo di tutti i sottoinsiemi di G, ad esempio, non è un suo sottoreticolo. Infatti, siano

$A, B \subset G$; allora, nel reticolo dei sottoinsiemi si ottiene che sup $\{A, B\} = A \cup B$, mentre nel reticolo dei sottogruppi, allora sup $\{A, B\} = \langle A, B \rangle$ che è il sottogruppo generato da A e B, e i due non coincidono.

Teorema 2.2.4. *Se M è un sottoinsieme di un reticolo completo L tale che, preso un qualsiasi sottoinsieme S di M, si ha che il minimo $\bigwedge S$ di S in L appartiene a M, allora M è un sottoreticolo inferiore completo.*

Dimostrazione. Sia S un sottoinsieme di M e sia S' l'insieme dei maggioranti di S in M. Per ipotesi, inf $S' \in M$. Notiamo che ogni $s \in S$ è un minorante di S' per come lo abbiamo costruito, e quindi $s \leq \inf S'$. Dunque inf S' è un maggiorante di S e, in particolare, è proprio l'estremo inferiore di S in M. Sappiamo inoltre che inf S è il minimo di S in M. Dunque M è un reticolo completo e il minimo di S in M e quello di S in L coincidono. □

Notiamo che, se G è un gruppo, il reticolo $L(G)$ dei sottogruppi di G è un esempio di sottoreticolo inferiore completo del reticolo di tutti i sottoinsiemi di G.

I seguenti risultati, che non dimostriamo, mostrano come i reticoli di sottogruppi e i loro sottoreticoli abbiano importanza generale.

Teorema 2.2.5 (Whitman)**.** *Ogni reticolo è isomorfo a un sottoreticolo di un reticolo di sottogruppi di un certo gruppo G.*

Teorema 2.2.6 (Pudlàk e Tuma)**.** *Ogni reticolo finito è isomorfo a un sottoreticolo del reticolo dei sottogruppi di un certo gruppo G finito.*

2.3 Reticoli di sottogruppi di composizione

Definizione 2.3.1. Un sottogruppo H di un gruppo G si dice *subnormale* in G se esistono un intero non negativo n e una serie

$$H = H_n \trianglelefteq H_{n-1} \trianglelefteq ... \trianglelefteq H_1 \trianglelefteq H_0 = G$$

di sottogruppi H_i di G tali che ogni H_i è un sottogruppo normale di H_{i-1}. In questo caso scriviamo $H \trianglelefteq\trianglelefteq G$.

Definizione 2.3.2. Diciamo che H è un *sottogruppo di composizione* di G se esiste una serie subnormale per H (come sopra) in cui tutti i gruppi quoziente H_i/H_{i+1} sono semplici, cioè non hanno sottogruppi normali propri e sono non banali. Chiamiamo n il tipo di H e chiamiamo la serie di 2.3.1 *serie di composizione* da G ad H di lunghezza n.
Osserviamo anche che una serie di composizione di sottogruppi è sempre subnormale, mentre il contrario non è sempre vero.

Definizione 2.3.3. Una serie subnormale

$$1 = H_m \trianglelefteq H_{m-1} \trianglelefteq ... \trianglelefteq H_1 \trianglelefteq H_0 = G$$

è un *raffinamento* di un'altra serie subnormale

$$1 = G_n \trianglelefteq G_{n-1} \trianglelefteq ... \trianglelefteq G_1 \trianglelefteq G_0 = G$$

se $G_0, ..., G_n$ è una sottosuccessione di $H_0, H_1, ..., H_m$. Un raffinamento è anche una serie subnormale che contiene ciascuno dei termini della serie originale.

Definizione 2.3.4. Data una serie di composizione come in 2.3.1, si dicono *fattori di composizione* i gruppi quoziente H_i/H_{i-1}.

Definizione 2.3.5. Due serie normali di un gruppo G di dicono *equivalenti* se esiste una biiezione tra i loro fattori di composizione tale che i fattori corrispondenti siano isomorfi.

Teorema 2.3.6 (Lemma di Zassenhaus)**.** *Siano $A \trianglelefteq A^\star$ e $B \trianglelefteq B^\star$ quattro sottogruppi di un gruppo G. Allora $A(A^\star \cap B) \trianglelefteq A(A^\star \cap B^\star)$ e $B(B^\star \cap A) \trianglelefteq B(B^\star \cap A^\star)$. Inoltre esiste un isomorfismo*

$$\sigma : \frac{A(A^\star \cap B^\star)}{A(A^\star \cap B)} \to \frac{B(B^\star \cap A^\star)}{B(B^\star \cap A)}$$

Dimostrazione. Poiché $A \trianglelefteq A^\star$, abbiamo che A è normalizzato da $A^\star \cap B^\star$ e quindi $A \cap B^\star = A \cap (A^\star \cap B^\star) \trianglelefteq A^\star \cap B^\star$. Allo stesso modo, otteniamo che $A^\star \cap B \trianglelefteq A^\star \cap B^\star$.
Sia ora $D = (A^\star \cap B)(A \cap B^\star)$. Per il Teorema 2.1.2 abbiamo che D è un sottogruppo normale di $A^\star \cap B^\star$.

Sia ora $x \in B(B^\star \cap A^\star)$ allora possiamo scrivere $x = bc$ con $b \in B$ e $c \in (B^\star \cap A^\star)$. Ora, definiamo una funzione $f\colon B(B^\star \cap A^\star) \to \frac{(A^\star \cap B^\star)}{D}$ tale che $f(x) = f(bc) = cD$. Verifichiamo che f sia ben posta.
Supponiamo quindi che $x = bc = b'c'$ con $b, b' \in B$ e $c, c' \in (A^\star \cap B^\star)$. Allora $c'c^{-1} = b'^{-1}b \in (B^\star \cap A^\star) \cap B = B \cap A^\star \leq D$. Dunque f è ben definita.
Verificare che f è suriettiva è immediato, e il suo nucleo è chiaramente $B(B^\star \cap A)$, infatti mostriamo che $bc \in \text{Ker } f$ se e solo se $c \in (A^\star \cap B)(A \cap B^\star)$. Allora scriviamo $c = b_1a_1$ con $b_1 \in B \leq (B \cap A^\star),\ a_1 \in (A \cap B^\star)$, dunque $c \in B(A \cap B^\star)$ e otteniamo che $bc \in B(A \cap B^\star)$. Quindi $bc \in \text{Ker } f$ implica che $bc \in A \cap B^\star$, dunque Ker $f \leq B(A \cap B^\star)$. L'altra inclusione è ovvia.
A questo punto possiamo concludere, grazie al primo teorema di isomorfismo, che $\frac{(A^\star \cap B^\star)}{D}$ è isomorfo a $\frac{B(B^\star \cap A^\star)}{B(B^\star \cap A)}$.
Osserviamo anche che, scambiando A e B otteniamo che $A(A^\star \cap B) \trianglelefteq A(A^\star \cap B^\star)$ e che $\frac{(A^\star \cap B^\star)}{D}$ è isomorfo a $\frac{A(A^\star \cap B^\star)}{A(A^\star \cap B)}$ componendo i due isomorfismi. □

Ora enunciamo e dimostriamo due importanti teoremi sui raffinamenti che saranno la base per le prossime dimostrazioni sulle serie di composizione.

Teorema 2.3.7 (di raffinamento di Schreier)**.** *Ogni coppia di serie subnormali di un qualsiasi gruppo G possiede dei raffinamenti equivalenti.*

Dimostrazione. Siano

$$1 = G_n \leq G_{n-1} \leq ... \leq G_0 = G$$

e

$$1 = H_m \leq H_{n-1} \leq ... \leq H_0 = G$$

due serie subnormali. Definiamo $G_{i,j} = G_{i+1}(G_i \cap H_j)$ per ogni $1 \leq j \leq m$ e osserviamo che

$$G_{i,j+1} = G_{i+1}(G_i \cap H_{j+1}) \leq G_{i+1}(G_i \cap H_j) = G_{i,j}$$

e notiamo inoltre che $G_{i,0} = G_i$, perché $H_0 = G$, e che $G_{i,m} = G_{i+1}$ in quanto $H_m = 1$.
Ora applichiamo il lemma di Zassenhaus ponendo $A = G_{i+1}$, $A^\star = G_i$, $B = H_{j+1}$ e $B^\star = H_j$ e a questo punto possiamo affermare che $G_{i,j+1} \trianglelefteq G_{i,j}$. Questo significa che la successione

$$1 \leq G_{n-1,m} \leq ... \leq G_{n-1,0} \leq ... \leq G_{0,m} \leq ... \leq G_{0,0}$$

è un raffinamento della prima serie subnormale che avevamo definito. Allo stesso modo, se definiamo gli $H_{i,j} = H_{i+1}(H_j \cap G_i)$ otteniamo che $H_{i+1,j} \leq H_{i,j}$ e che

$$1 \leq H_{n-1,m} \leq ... \leq H_{n-1,0} \leq ... \leq H_{0,m} \leq ... \leq H_{0,0}$$

è un raffinamento della seconda serie che abbiamo definito.
Ora, cerchiamo una biiezione che porti i fattori del primo raffinamento in quelli del secondo, e quindi poniamo

$$\sigma\left(\frac{G_{i,j}}{G_{i,j+1}}\right) = \frac{H_{i,j}}{H_{i+1,j}}$$

Osserviamo che σ è biiettiva per definizione. Utilizziamo il lemma di Zassenhaus, ponendo $A^\star, A, B, B^\star$ come sopra. Otteniamo quindi che i

fattori corrispondenti dei due raffinamenti sono tra loro isomorfi, e dunque i raffinamenti sono equivalenti. □

Teorema 2.3.8 (di Jordan-Holder)**.** *Due serie di composizione di un gruppo G sono sempre equivalenti.*

Dimostrazione. Consideriamo due serie di composizione; poiché in particolare esse sono subnormali, esse possiedono raffinamenti equivalenti, e siccome sono serie subnormali di lunghezza massima, allora non hanno raffinamenti propri, e quindi possiamo concludere. □

2.4 Reticolo dei sottogruppi di composizione

In questa sezione, ci occuperemo di dimostrare che l'insieme di tutti i sottogruppi di composizione di G è un sottoreticolo del reticolo dei sottogruppi $L(G)$. Per farlo, ci avvaliamo dei seguenti risultati.

Proposizione 2.4.1. *Sia $A \trianglelefteq G$ e sia $B_{i+1} \trianglelefteq B_i \leq G$. Allora si ha che $A \vee B_{i+1} \trianglelefteq A \vee B_i$, cioè $AB_{i+1} \trianglelefteq AB_i$.*

Dimostrazione. Osserviamo che AB_{i+1} è un sottogruppo grazie a 2.1.2, inoltre si ha che $A \vee B_{i+1} = AB_{i+1}$ per la Proposizione 2.2.2. Quindi è sufficiente mostrare che preso un elemento $xy \in A \vee B_{i+1}$, cioè tale che

$x \in A$ e $y \in B_{i+1}$, si ha che $(xy)^{ab_i} \in A \vee B_{i+1}$ con $a \in A$ e $b_i \in B_i$. Allora abbiamo che

$$(ab_i)^{-1}(xy)ab_i = (ab_i)^{-1}x(ab_i)(ab_i)^{-1}yab_i = (x^{ab_i})b_i^{-1}a^{-1}(ya)y^{-1}yb_i =$$

$$= (x^{ab_i})b_i^{-1}a^{-1}yay^{-1}b_i(b_i^{-1}yb_i) = (x^{ab_i})(a^{-1}yay^{-1})^{b_i}y^{b_i}$$

con $x^{ab_i} \in A$, $y^{b_i} \in B_{i+1}$ perché B_{i+1} è normalizzato da B_i e $(a^{-1}yay^{-1}) \in A$, perché $a^{-1} \in A$ e $yay^{-1} \in A$ in quanto è il coniugato di y e A è normale. Dunque abbiamo ottenuto la tesi. □

Teorema 2.4.2. *Sia H un sottogruppo di composizione di tipo n in G tale che $H < K < G$ e $K \trianglelefteq \trianglelefteq G$. Allora esistono due serie di composizione di lunghezza minore di n rispettivamente da G a K e da K a H.*

Dimostrazione. Sia

$$H = H_n \trianglelefteq H_{n-1} \trianglelefteq ... \trianglelefteq H_1 \trianglelefteq H_0 = G$$

una serie di composizione da H a G e sia

$$K = K_m \trianglelefteq K_{m-1} \trianglelefteq ... \trianglelefteq K_0 = G$$

una serie di composizione da K a G. Allora la serie

$$H = K \cap H_n \trianglelefteq K \cap H_{n-1} \trianglelefteq ... \trianglelefteq K \cap H_1 \trianglelefteq K \trianglelefteq K_{m-1} \trianglelefteq ... \trianglelefteq K_0 = G$$

è una serie subnormale da G ad H. Allora, per il teorema di raffinamento di Schreier, le due serie da H a G possiedono dei raffinamenti equivalenti.

Nella prima serie di composizione non ci sono raffinamenti propri (cioè di lunghezza minore di n), dunque anche l'altra serie deve avere un raffinamento di lunghezza n che a sua volta non possiede raffinamenti propri. Poiché $H < K < G$, le due serie da H a K e da K a G sono serie di composizione e devono avere lunghezza minore di n. □

Nel prossimo teorema, usiamo la notazione $A \wedge B$ per chiarezza concettuale, in quanto $A \cap B = A \wedge B$ nel caso di sottogruppi.

Teorema 2.4.3 (di Wielandt)**.** *Sia G gruppo. L'insieme $R(G)$ di tutti i sottogruppi di composizione è un sottoreticolo del reticolo dei sottogruppi $L(G)$.*

Dimostrazione. Siano $A, B \in R(G)$. Allora esistono le serie di composizione

$$A = A_m \trianglelefteq A_{m-1} \trianglelefteq ... \trianglelefteq A_1 \trianglelefteq A_0 = G$$

e

$$B = B_n \trianglelefteq B_{n-1} \trianglelefteq ... \trianglelefteq B_1 \trianglelefteq B_0 = G$$

rispettivamente da G ad A e da G a B. Usiamo l'induzione su $\min(n, m)$ per dimostrare che $A \wedge B \in R(G)$.
Assumiamo quindi che $m \leq n$. Se $m = 0$ allora $A = G$ e quindi $A \wedge B = B \in R(G)$ per ipotesi, quindi non c'è niente da dimostrare. Supponiamo quindi che $m \geq 1$ e studiamo prima A_1. Osserviamo che

$$A_1 \leq A_1 \vee B = A_1 \vee B_n \trianglelefteq ... \trianglelefteq A_1 \vee B_0 = G$$

e che G/A_1 è semplice (per definizione di serie di composizione), allora abbiamo che $A_1 \vee B = A_1$ oppure $A_1 \vee B = G$. Consideriamo $B_1 \trianglelefteq B_0 = G$, allora abbiamo che $A_1 \vee B_1 = A_1$ oppure $A_1 \vee B_1 = G$, e dunque nel primo caso $A_1 \leq A_1 \vee B \leq A_1 \vee B_1 = A_1$ e quindi $A_1 \vee B = A_1$. Dunque otteniamo che $A_1 \wedge B = B$.
Nel secondo caso $A_1 \vee B_1 = G$, e abbiamo grazie alla Proposizione 2.4.1 che A_1B_2 è normale in G. Allora si ha che $A_1B_2 = A_1$ oppure $A_1B_2 = G$. Nel primo caso, otteniamo che $A_1 \wedge B = A_1$ come nel caso precedente. Nel secondo caso, osserviamo che A_1B_3 è normale in G. Iterando questo processo n volte otteniamo che $A_1 \vee B_n = A_1 \vee B = G$. Nel secondo caso, si ha che $A_1 \wedge B \trianglelefteq B$. Dunque, possiamo applicare il secondo teorema di isomorfismo, in quanto $G = A_1 \vee B = A_1B$ e $A_1 \wedge B = A_1 \cap B$, e dunque otteniamo che $B/A_1 \wedge B \simeq G/A_1$ e quindi è semplice. In entrambi i casi, $A_1 \wedge B \in R(G)$ e per il teorema precedente abbiamo che $A_1 \wedge B \in R(A_1)$. Per ipotesi induttiva $A \wedge B = A \wedge (A_1 \wedge B) \in R(A_1)$, e allora $A \wedge B \in R(G)$ dato che G/A_1 è semplice.
Ora l'idea è quella di usare l'induzione su $(\min(n,m), \max(n,m))$ per far vedere che $A \vee B \in R(G)$. Come prima, per $m = n = 0$ è banale, per cui supponiamo che $n, m \geq 1$ e notiamo che l'estremo superiore di due sottogruppi di composizione rispettivamente di tipo r e s è ancora un sottogruppo di composizione per tutti gli r, s con $r \leq s < \max(n,m)$ oppure con $s = \max(n,m)$ e $r < \min(n,m)$.
Supponiamo innanzitutto che A non sia normale in $A \vee B$, allora esiste $b \in B$ tale che $A^b \neq A$, perché sappiamo che $A \trianglelefteq A \vee B$ se e solo se $A^b = A$ per ogni $b \in B$. Ricordando che $A \leq A_1 \trianglelefteq G$, notiamo che $A^b \leq A_1^b \leq A_1$, dunque esistono due serie di composizione di lunghezza $m-1 < \max(n,m)$

rispettivamente da A_1 ad A e da A_1 ad A^b. A questo punto possiamo applicare l'ipotesi induttiva e affermare che $A \vee A^b \in R(A_1)$ e quindi $A \vee A^b \trianglelefteq \trianglelefteq G$ in quanto per il teorema precedente esiste una serie di composizione di lunghezza minore di m da G ad $A \vee A^b$. Dunque possiamo dire che $A \vee B = (A \vee A^b) \vee B \in R(G)$. Analogamente, se B non è normale in $A \vee B$, otteniamo lo stesso risultato.
Ora possiamo supporre $A \trianglelefteq A \vee B$ e che $B \trianglelefteq A \vee B$. Nel primo caso, di nuovo, per ipotesi induttiva, $A_{m-1} \vee B \in R(G)$. Se $A_{m-1} \vee B \neq G$ allora per il teorema precedente esistono una serie di composizione di lunghezza minore di m e una serie di composizione di lunghezza minore di n rispettivamente da $A_{m-1} \vee B$ ad A e da $A_{m-1} \vee B$ a B. Dunque per ipotesi induttiva $A \vee B \in R(A_{m-1} \vee B)$ e dunque $A \vee B \in R(G)$.
Infine supponiamo che $A_{m-1} \vee B = G$, e allora $A \trianglelefteq G$ poiché A è normalizzato da A_{m-1} e da B. Analogamente, possiamo supporre $A \vee B_{n-1} = G$, e otteniamo che $B \trianglelefteq G$ e dunque $A \vee B \trianglelefteq G$ e per il Teorema 2.4.2 si ha che $A \vee B \in R(G)$. □

Concludendo il discorso sulle serie di composizione, abbiamo mostrato che in un gruppo G con una serie di composizione, ogni sottogruppo subnormale è un sottogruppo di composizione. Quindi in questi gruppi (in particolare quelli finiti), sottogruppi subnormali e sottogruppi di composizione coincidono. Per questa ragione $R(G)$ è definito anche il *reticolo dei sottogruppi subnormali di* G.

Capitolo 3

Teorema di Ore

3.1 Reticoli distributivi

Definizione 3.1.1. Un reticolo L è detto *distributivo* se per ogni $x, y, z \in L$ vale la proprietà distributiva, cioè se

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \tag{3.1}$$

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \tag{3.2}$$

Osservazione 3.1.2. Poiché la distributività è una proprietà definita componente per componente, i sottoreticoli e i prodotti diretti di reticoli distributivi sono a loro volta distributivi. Inoltre, un reticolo L è distributivo anche se soddisfa una sola tra (3.1) e (3.2).
Infatti, se vale (3.1) abbiamo che

$$(x \wedge y) \vee (x \wedge z) = ((x \wedge y) \vee x) \wedge (x \wedge y) \vee z) =$$

$$= x \wedge (z \vee (x \wedge y)) = x \wedge ((z \vee x) \wedge (z \vee y)) = x \wedge (y \vee z)$$

e analogamente si può arrivare a (3.1) partendo da (3.2).

3.2 Gruppi localmente ciclici

Definizione 3.2.1. Sia $n \in \mathbb{N} \cup \{\infty\}$. Denotiamo il gruppo ciclico di ordine n come C_n. Sia $C_n = \langle g \rangle$. Se $n = \infty$ osserviamo che i sottogruppi di $\langle g \rangle$ sono tutti e soli i sottogruppi del tipo $\langle g^r \rangle$ con $r \in \mathbb{N}$. Se $n \in \mathbb{N}$, allora i sottogruppi di $\langle g \rangle$ sono tutti e soli del tipo $\langle g^r \rangle$ con r che divide n. Un tale sottogruppo ha ordine r/n.

Osservazione 3.2.2. Sia T_n il reticolo dei divisori di n come definito in precedenza. Se definiamo $\sigma : T_n \to L(\langle g \rangle)$ tale che $r^\sigma = \langle g^r \rangle$ per ogni $r \in T_n$, allora abbiamo che σ è biiettiva. Inoltre, presi $r, s \in T_n$, abbiamo che $r \leq s$ se e solo se s divide r cioè se e solo se $\langle g^r \rangle \subseteq \langle g^s \rangle$. Allora σ è un isomorfismo e quindi $L(C_n) \simeq T_n$.

Ora diamo la definizione di gruppo localmente ciclico, che permetterà di enunciare il Teorema di Ore.

Definizione 3.2.3. Un gruppo G è detto *localmente ciclico* se ogni sottoinsieme finito di G genera un sottogruppo ciclico. Equivalentemente, possiamo dire che G è localmente ciclico se $\langle a, b \rangle$ è ciclico per ogni coppia a, b di elementi di G. In particolare, ogni gruppo localmente ciclico è abeliano.

Osservazione 3.2.4. Due esempi di gruppo localmente ciclico sono $\mathbb{Q}$ e il gruppo $\mathbb{Q}/\mathbb{Z}$. Vediamo la dimostrazione per $\mathbb{Q}$. Siano $r, s, p, q \in \mathbb{N}$ tali che $s \neq 0$, $q \neq 0$ e tali che MCD $(r, s) =$ MCD $(p, q) = 1$. Allora $\langle \frac{r}{s}, \frac{p}{q} \rangle = \{m\frac{r}{s} + n\frac{p}{q} \mid m, n \in \mathbb{Z}\} = \{\frac{rqm+psm}{sq} \mid m, n \in \mathbb{Z}\} = \langle \frac{\text{MCD } (rq,ps)}{sq} \rangle$, che è esattamente l'insieme dei multipli di MCD (rq, ps), e dunque abbiamo ottenuto la tesi. Per= $\mathbb{Q}/\mathbb{Z}$ basta prendere la proiezione π di $\mathbb{Q}$ sul quoziente, e osservare che $\pi(\langle \frac{r}{s}, \frac{p}{q} \rangle) = \pi(\langle \frac{\text{MCD } (rq,ps)}{sq} \rangle)$, che è un gruppo ciclico.

Definizione 3.2.5. Chiamiamo *centro* di un gruppo G l'insieme $Z(G) = \{z \in G; gz = zg \text{ per ogni } g \in G\}$ cioè è l'insieme di tutti gli elementi di G che commutano con ogni elemento di G.

Prima di enunciare il teorema di Ore, diamo alcuni risultati utili alla comprensione della dimostrazione.

Proposizione 3.2.6. *Sia G un gruppo e sia $N \leq Z(G)$ tali che G/N è ciclico. Allora G è commutativo.*

Dimostrazione. Sia $G/N = \langle gN \rangle$, allora $G/N = \{g^i N, i \in \mathbb{Z}\}$. Siano $x_1, x_2 \in G$ con $x_1 \in g^j N$ e $x_2 \in g^k N$, allora essi si possono scrivere come $x_1 = g^j n_j$ e $x_2 = g^k n_k$ con $n_j, n_k \in N$. Dunque

$$x_1 x_2 = g^j n_j g^k n_k = g^j g^k n_j n_k = g^k g^j n_k n_j = g^k n_k g^j n_j = x_2 x_1$$

dove abbiamo usato che $N \leq Z(G)$ e quindi tutti i suoi elementi commutano con quelli di G. □

Definizione 3.2.7. Sia G un gruppo commutativo. Poniamo $G^n = \{g^n \mid g \in G\}$. Osserviamo che G^n è un sottogruppo.

Proposizione 3.2.8. *Siano U, V due gruppi e sia $G = U \times V$. Sia p un primo. Allora $G^p = U^p \times V^p$ e in particolare $G/G^p \simeq U/U^p \times V/V^p$*

Dimostrazione. Osserviamo che $G^p = \{(x_1, x_2)^p \mid x_1 \in U, x_2 \in V\} = \{(x_1^p, x_2^p) \mid x_1 \in U, x_2 \in V\} = U^p \times V^p$. Per dimostrare la seconda affermazione è sufficiente considerare $\pi : U \times V \to U/U^p \times V/V^p$ tale che $\pi(u, v) = (uU^p, vV^p)$ e studiarne il nucleo in modo da poter applicare il primo teorema di isomorfismo. Allora Ker $\pi = \{(x, y);\ x \in U^p, y \in V^p\} = U^p \times V^p$ e quindi possiamo concludere. □

Proposizione 3.2.9. *Sia G un gruppo abeliano e sia p un primo. Allora G/G^p è uno spazio vettoriale sul campo con p elementi.*

Dimostrazione. Definiamo l'applicazione $\sigma : \mathbb{Z}/p\mathbb{Z} \times G/G^p \to G/G^p$ tale che $\sigma([z], gG^p) = (g^z G^p)$. Osserviamo che σ è ben definita. in quanto se $[z_1] = [z_2]$, allora $z_1 - z_2 = kp$ con $k \in \mathbb{Z}$, e quindi $g^{z_1 - z_2} = g^{kp} \in G^p$ e allora $g^{z_1} G^p = g^{z_2} G^p$. Con questa struttura, G/G^p gode di tutte le proprietà degli spazi vettoriali, per cui risulta uno spazio vettoriale su $\mathbb{F}_p \simeq \mathbb{Z}_p$. □

Ricordiamo il teorema di struttura dei gruppi abeliani finitamente generati, che ci permetterà di enunciare le prossime proposizioni.

Teorema 3.2.10. *Ogni gruppo abeliano finito è isomorfo alla somma diretta di gruppi ciclici i cui ordini sono potenze di numeri primi.*

Proposizione 3.2.11. *Sia G un gruppo abeliano $G = \langle a, b\rangle$. Sia G prodotto diretto di gruppi ciclici $C_{d_1} \times ... \times C_{d_k} \times Z_1 \times ... \times Z_s$ con C_{d_i} gruppo ciclico finito di ordine d_i con $d_1|d_2|...|d_k$ e Z_j gruppi ciclici infiniti. In questo caso, si ha che $k + s \leq 2$.*

Dimostrazione. Sia p un primo che divide d_1. Definiamo come nel precedente teorema $(C_{d_1} \times ... \times C_{d_k} \times Z_1 \times ... \times Z_s)^p = \{(x_1^p, x_2^p, ..., x_k^p, y_1^p, ..., y_s^p)$ con $x_i \in C_{d_i}, y_j \in Z_j\}$ e otteniamo che

$$G/G^p \simeq C_{d_1}/C_{d_1}^p \times ... \times C_{d_k}/C_{d_k}^p \times Z_1/Z_1^p \times ... \times Z_s/Z_s^p \quad (\star)$$

grazie alla Proposizione 3.2.8. Poiché $G = \langle a, b\rangle$, anche G/G^p è generato da due elementi e ha dimensione al più due. Ora, osserviamo che G/G^p è uno spazio vettoriale sul campo con p elementi, come dal teorema precedente, di dimensione al più 2. Inoltre osserviamo che $C_{d_i}/C_{d_i}^p$ è uno spazio vettoriale non banale di dimensione 1, poiché $C_{d_i}^p$ è un sottogruppo proprio di C_{d_i} per ogni i in quanto p divide ogni d_i. La stessa cosa si può dire per Z_j. Dunque nel membro a destra in $(\star)$ compare il prodotto diretto di $k + s$ spazi vettoriali di dimensione 1. Segue che $k + s \leq 2$. □

Ora siamo pronti per enunciare e dimostrare il Teorema di Ore.

Teorema 3.2.12 (Teorema di Ore)**.** *Il reticolo dei sottogruppi di un gruppo G è distributivo se e solo se G è localmente ciclico.*

Dimostrazione. Supponiamo prima che $L(G)$ sia distributivo. Siano $a, b \in G$. Dobbiamo mostrare che $\langle a, b\rangle$ è ciclico. Poiché $\langle a\rangle \wedge \langle b\rangle$ è centralizzato da a e da b, allora $\langle a\rangle \wedge \langle b\rangle \leq Z(\langle a, b\rangle)$, con $Z(\langle a, b\rangle)$ centro di $\langle a, b\rangle$. Osserviamo anche che $\langle ab\rangle \vee \langle a\rangle = \langle a, b\rangle = \langle ab\rangle \vee \langle b\rangle$.
Allora, poiché $L(G)$ è distributivo, abbiamo che

$$\langle ab\rangle \vee (\langle a\rangle \wedge \langle b\rangle) = (\langle ab\rangle \vee \langle a\rangle) \wedge (\langle ab\rangle \vee \langle b\rangle) = \langle a, b\rangle$$

Utilizziamo il secondo teorema di isomorfismo 2.1.6, con $U = \langle ab\rangle$ e $V = \langle a\rangle \wedge \langle b\rangle$. Otteniamo quindi che

$$\langle a, b\rangle / \langle a\rangle \wedge \langle b\rangle \simeq \langle ab\rangle / \langle ab\rangle \wedge (\langle a\rangle \wedge \langle b\rangle)$$

e dunque, poiché $\langle ab\rangle$ è un gruppo ciclico e ogni suo quoziente è ciclico, allora $\langle a, b\rangle / \langle a\rangle \wedge \langle b\rangle$ è ciclico. Inoltre, $\langle a, b\rangle$ è un gruppo abeliano, in quanto è estensione ciclica di un sottogruppo centrale, per la Proposizione 3.2.6.
Osserviamo inoltre che per il teorema precedente esistono $c, d \in G$ tali che $\langle a, b\rangle = \langle c\rangle \times \langle d\rangle$. Anche in questo caso $\langle c, d\rangle / \langle c\rangle \wedge \langle d\rangle$ è ciclico. Tuttavia, qui abbiamo che $\langle c\rangle \wedge \langle d\rangle = 1$, quindi anche $\langle a, b\rangle = \langle c, d\rangle$ è ciclico.
Vediamo ora l'implicazione inversa. Supponiamo che G sia localmente ciclico, e siano $A, B, C \in L(G)$. Basta mostrare che vale la (3.1) per concludere, o, in alternativa, poiché G è abeliano e possiamo usare la Proposizione 2.2.2, che $A(B \wedge C) = AB \wedge AC$. Ovviamente $A(B \wedge C) \leq AB \wedge AC$. Mostriamo l'inclusione inversa. Sia $x \in AB \wedge AC$, allora $x = a_1 b = a_2 c$ con $a_1, a_2 \in A, b \in B, c \in C$.
Poiché G è localmente ciclico, allora esiste $g \in G$ tale che $\langle a_1, a_2, b, c\rangle =$

$\langle g\rangle$. Allora mostriamo che $a_1b = a_2c$ implica che

$$\langle g\rangle = (A \wedge \langle g\rangle)(B \wedge \langle g\rangle) = (A \wedge \langle g\rangle)(C \wedge \langle g\rangle)$$

Banalmente $\langle g\rangle \supseteq (A \wedge \langle g\rangle)(B \wedge \langle g\rangle)$, l'altra inclusione invece si ottiene mostrando che $g \in (A \wedge \langle g\rangle)(B \wedge \langle g\rangle)$.
Sappiamo già che $g = a_1^r\ a_2^s\ b^k\ c^t$ e osserviamo che $c = a_1ba_2^{-1}$, allora $c \in (A \wedge \langle g\rangle)(B \wedge \langle g\rangle)$ in quanto $b \in B$ e $a_1, a_2 \in A$, e quindi

$$g = a_1^{r+t}\ a_2^{s-t}\ b^{k+t}\ \in\ (A \wedge \langle g\rangle)(B \wedge \langle g\rangle)$$

Analogamente, ponendo $b = a_2ca_1^{-1}$ si ha che $g \in (A \wedge \langle g\rangle)(C \wedge \langle g\rangle)$.
Ora, se uno tra i tre sottogruppi $A \wedge \langle g\rangle$, $B \wedge \langle g\rangle$, $C \wedge \langle g\rangle$ è il gruppo banale, allora abbiamo due casi: $x = b = c \in B \wedge C$ oppure $x \in A$. In entrambi i casi, abbiamo che $x \in A(B \wedge C)$. Supponiamo allora che i tre sottogruppi siano tutti non banali, e siano $A \wedge \langle g\rangle = \langle g^n\rangle$, $B \wedge \langle g\rangle = \langle g^r\rangle$, $C \wedge \langle g\rangle = \langle g^s\rangle$. Allora si ha che $g = g^{nk_1}g^{rk_2} = g^{nk_3}g^{sk_4}$.
Consideriamo il caso $g = g^{nk_1}g^{rk_2}$. Se $\langle g\rangle$ ha ordine m, allora $n|m$ e $r|m$ $1 \equiv nk_1 + rk_2$ modulo m. Mostriamo che $\mathrm{MCD}(n, r) = 1$. infatti, sia $\mathrm{MCD}(n, r) = d$; allora, poiché $n|m$ e $r|m$, dunque $d|m|nk_1 + rk_2 - 1$, inoltre $d|n$ e $d|r$ e quindi $d|1$ e necessariamente $d = 1$.
Se $\langle g\rangle$ è infinito, allora in questo caso $1 = nk_1 + rk_2$ allora $\mathrm{MCD}(n, r) = 1$ perché se per assurdo $\mathrm{MCD}(n, r) = d > 1$, allora $d|nk_1 + rk_2 = 1$ e dunque di nuovo $d = 1$. Analogamente possiamo applicare lo stesso procedimento per ottenere che $\mathrm{MCD}(n, s) = 1$, e dunque $\mathrm{MCD}(n, rs) = 1$ e inoltre $\langle g\rangle = \langle g^n\rangle\langle g^{rs}\rangle = (A \wedge \langle g\rangle)(B \wedge C \wedge \langle g\rangle) \leq A(B \wedge C)$ e di nuovo questo significa che $x \in A(B \wedge C)$, e quindi otteniamo che $AB \wedge AC \leq A(B \wedge C)$ e dunque sono uguali. A questo punto possiamo concludere. □

3.3 Caratterizzazione dei reticoli di gruppi ciclici

Usando il Teorema di Ore non è difficile caratterizzare la classe dei gruppi ciclici. Vediamo un teorema che è una sua importante conseguenza, ricordando che il reticolo di un gruppo ciclico C_n è isomorfo a T_n e che il reticolo di un gruppo ciclico C_∞ è isomorfo a T_∞.

Teorema 3.3.1. *Un gruppo G è ciclico se e solo se il suo reticolo di sottogruppi $L(G)$ è distributivo e soddisfa la condizione di massimalità.*

Dimostrazione. Non è difficile provare che, se $L(G)$ soddisfa la condizione di massimalità, allora G è finitamente generato. Infatti, una definizione equivalente di condizione di massimalità è che non esistano successioni infinite di elementi $x_1, x_2...$, tali che $x_1 < x_2 < ....$ Dunque G deve essere finitamente generato. Inoltre, poiché $L(G)$ è distributivo, allora, per il teorema di Ore, G è localmente ciclico. Dunque, abbiamo ottenuto che G è localmente ciclico e finitamente generato, dunque è ciclico.
Viceversa, se G è ciclico. allora otteniamo che $L(G)$ è distributivo per il teorema di Ore (infatti se G è ciclico, in particolare è localmente ciclico), e inoltre, se $1 < H \leq G$, allora l'intervallo $[G, H]$ è finito, in quanto se G ha ordine n, l'affermazione è banalmente vera. Se G ha ordine infinito, invece, sappiamo che i suoi sottogruppi H sono del tipo $\langle g^r \rangle$ con $r \in \mathbb{N}$. Dunque i sottogruppi K tali che $H \leq K \leq G$ sono in corrispondenza biunivoca con i sottogruppi del quoziente G/H, che ha ordine necessariamente finito, e dunque i suoi sottogruppi sono in numero finito, allora anche in questo

caso l'intervallo $[G, H]$ è finito, e quindi $L(G)$ soddisfa la condizione di massimalità. □

Teorema 3.3.2. *Sia G un gruppo. Allora $G \simeq C_\infty$ se e solo se $L(G) \simeq T_\infty$*

Dimostrazione. Se $G \simeq C_\infty$ allora $L(G) \simeq T_\infty$ per l'osservazione 3.2.2. Viceversa, se $L(G) \simeq T_\infty$, allora $L(G) \simeq L(C_\infty)$, inoltre L è distributivo, e soddisfa la condizione di massimalità. G è ciclico, e dunque $|G|$ è infinita. □

Osservazione 3.3.3. In questo modo il gruppo ciclico infinito C_∞ è determinato dal suo reticolo dei sottogruppi, cioè è l'unico gruppo tale che il suo reticolo dei sottogruppi è isomorfo a $L(C_\infty)$. Per gruppi ciclici finiti il discorso è diverso, in quanto per $m, n \in \mathbb{N}$ i reticoli T_m e T_n possono essere isomorfi tra loro anche se $m \neq n$, infatti, sia $m = p_1^{m_1} \cdot ... \cdot p_r^{m_r}$ la decomposizione di m in fattori primi. Allora ogni divisore di m è della forma $p_1^{k_1} \cdot ... \cdot p_r^{k_r}$ con $k_i \leq m_i$ per $i = 1, ..., r$. La mappa σ definita da

$$(p_1^{m_1} \cdot ... \cdot p_r^{m_r})^\sigma = (p_1^{k_1}, ..., p_r^{k_r})$$

è un isomorfismo da T_m al prodotto diretto dei $T_{p_i^{k_i}}$ come nella Proposizione 1.4.3, che sono tutte catene di lunghezza m_i. Inoltre, T_m contiene esattamente r antiatomi, che sono $p_1, ..., p_r$ e per ogni p_i esso contiene esattamente una catena di massima lunghezza m_i tra 1 e p_i. Quindi, se $n \in \mathbb{N}$ tale che $T_m \simeq T_n$ e sia τ l'isomorfismo tra i due reticoli, allora abbiamo che i p_i^τ sono tutti primi distinti e $n = (p_1^\tau)^{m_1} \cdot ... \cdot (p_r^\tau)^{m_r}$.

Teorema 3.3.4. *Siano $n_1, ..., n_r \in \mathbb{N}$. Il gruppo G è ciclico di ordine $p_1^{n_1} \cdot ... \cdot p_r^{n_r}$ con p_i primi distinti se e solo se $L(G)$ è prodotto diretto di catene di lunghezza $n_1, ..., n_r$.*

Dimostrazione. Se G è un gruppo ciclico di ordine $m = p_1^{n_1} \cdot ... \cdot p_r^{n_r}$, allora grazie alla Proposizione 1.4.3 abbiamo che $L(G) = T_m$ è prodotto diretto di catene di lunghezza $n_1, ..., n_r$. Viceversa, supponiamo che $L(G) \simeq T_{m_1}$ sia distributivo e finito. Allora, si ha che G è ciclico e dunque $T_{m_1} \simeq L(G) \simeq T_{|G|}$ e quindi $|G| = p_1^{n_1} \cdot ... \cdot p_r^{n_r}$ con p_i primi distinti. □

Teorema 3.3.5. *Siano $n_1, ..., n_r \in \mathbb{N}$ e p_i primi distinti. Se G un gruppo ciclico di ordine $p_1^{n_1} \cdot ... \cdot p_r^{n_r}$ e sia G' un altro gruppo. Allora abbiamo che $L(G') \simeq L(G)$ se e solo se G' è ciclico di ordine $q_1^{n_1} \cdot ... \cdot q_r^{n_r}$, dove q_i sono primi distinti.*

Dimostrazione. Segue immediatamente dal Teorema 3.3.4. □

3.4 Reticoli modulari

Definizione 3.4.1. Un reticolo L si dice *modulare* se per ogni $x, y, z \in L$ vale la seguente proprietà:

$$\text{Se } x \leq y \text{ allora } x \vee (y \wedge z) = (x \vee y) \wedge z \tag{3.3}$$

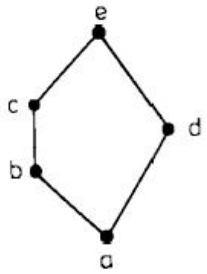
Osservazione 3.4.2. Sia L un reticolo e siano $x, y, z \in L$. Allora valgono le seguenti affermazioni:

1. Se $x \leq z$ allora $x \leq (x \vee y) \wedge z$ e $y \wedge z \leq (x \vee y) \wedge z$ e dunque $x \vee (y \wedge z) \leq (x \vee y) \wedge z$ vale in ogni reticolo.

2. Ogni reticolo distributivo è modulare, infatti se L distributivo e $x \leq z$, allora $x \vee z = z$ e quindi $x \vee (y \wedge z) = (x \vee y) \wedge (x \wedge z) = (x \vee y) \wedge z$

3. Se L è modulare, allora $x \vee (y \wedge (x \vee z)) = (x \vee y) \wedge (x \vee z)$ poiché $x \leq x \vee z$. Al contrario, se questa equazione vale in L, allora $x \leq z$ implica che $x \vee z = z$ e dunque $x \vee (y \wedge z) = (x \vee y) \wedge z$. Questo mostra che la modularità può essere definita usando un'identità. Quindi sottoreticoli e prodotti diretti di reticoli modulari, sono a loro volta modulari.

Osserviamo infine che l'unico reticolo non modulare con 5 o meno elementi è E_5 come nella figura. Dunque è doveroso enunciare il prossimo teorema.



Teorema 3.4.3. *Un reticolo L è modulare se e solo se non contiene un sottoreticolo isomorfo ad E_5.*

Dimostrazione. Se il reticolo L è modulare, allora ogni suo sottoreticolo è modulare e quindi non può essere isomorfo a E_5. Viceversa, dobbiamo mostrare che ogni reticolo L che non è modulare contiene un sottoreticolo isomorfo a E_5. Dunque, poiché L non è modulare, allora esistono $x, y, z \in L$ tali che se $x \leq z$, allora $x \vee (y \wedge z) < (x \vee y) \wedge z$. Allora, siano $a = y \wedge z$, $b = x \vee (y \wedge z)$, $c = (x \vee y) \wedge z$, $d = y$ ed $e = x \vee y$ e sia $S = \{a, b, c, d, e\}$. Allora otteniamo che $a \leq b < c \leq e$ e anche $a \leq d \leq e$. Inoltre,

$$c \wedge d = (x \vee y) \wedge z \wedge y = z \wedge y = a \quad \text{mentre} \quad b \vee d = x \vee (y \wedge z) \vee y = x \vee y = e$$

Da questo segue che $b \wedge d = a$ e che $c \vee d = e$. Dunque abbiamo che S è un sottoreticolo di L e che $b \leq c$ e $b \vee (d \wedge c) = b \neq c = (b \vee d) \wedge c$. Dunque S non è modulare e poiché tutti gli altri reticoli con al più 5 elementi sono modulari, dunque $S \simeq E_5$ □

3.5 Sottogruppi modulari e permutabili

Definizione 3.5.1. Diciamo che un elemento m del reticolo L è *modulare* in L e scriviamo $m \ mod \ L$ se

$$x \vee (m \wedge z) = (x \vee m) \wedge z \text{ per ogni } x, z \in L \text{ tali che } x \leq z \tag{3.4}$$

$$m \vee (y \wedge z) = (m \vee y) \wedge z \text{ per ogni } y, z \in L \text{ tali che } m \leq z \tag{3.5}$$

Un sottogruppo M di un gruppo G è detto *modulare* in G se M è modulare in $L(G)$ e scriviamo $M \ mod \ G$. Si osservi che un reticolo L è modulare se

e solo se ogni suo elemento è modulare in L.

Ora enunciamo un altro teorema di Ore, questa volta riguardante i sottogruppi modulari.

Teorema 3.5.2 (Ore)**.** *Sia G un gruppo. Allora se $N \trianglelefteq G$ si ha che $NH = HN$ per ogni $H \leq G$. Inoltre, se $M \leq G$ è tale che $MH = HM$ per ogni $H \leq G$ allora M è modulare in G.*

Dimostrazione. Se $N \trianglelefteq G$, allora abbiamo che $Nx = xN$ per ogni $x \in G$, e in particolare anche per ogni $x \in H$ in quanto $H \leq G$, dunque la prima affermazione è vera. Ora, consideriamo $X \leq Z \leq G$. Allora abbiamo che $X \vee (M \wedge Z) \leq (X \vee M) \wedge Z$. Dobbiamo mostrare l'inclusione inversa in modo da ottenere (3.4). Allora, sia $g \in (X \vee M) \wedge Z$. Poiché $X \vee M = XM$ per la Proposizione 2.2.2, allora esistono $x \in X$ e $m \in M$ tali che $g = xm$. Ora, poiché $X \leq Z$, allora si ha che $m = x^{-1}g$ e dunque $m \in Z$ e dunque otteniamo che $g = xm \in X \vee (M \wedge Z)$. Dunque abbiamo ottenuto l'uguaglianza.
Mostriamo ora in maniera analoga che vale la (3.5). Siano $Y, Z \leq G$ con $M \leq Z$. Allora, si ha che $M \vee (Y \wedge Z) \leq (M \vee Y) \wedge Z$. Sia $g = ym \in (M \vee Y) \wedge Z$, allora poiché $m \in M \leq Z$ si ha che $y \in Z$, dunque $g \in M \vee (Y \wedge Z)$ e dunque vale anche la (3.5). Allora abbiamo che M è modulare in G. □

Definizione 3.5.3. Un sottogruppo M di G è detto *permutabile* in G (e scriviamo M *per* G) se $MH = HM$ per ogni sottogruppo H di G.

Questi sottogruppi sono stati introdotti da Ore, che li ha chiamati *quasinormali*. Si osservi che il precedente teorema afferma proprio che un sottogruppo normale è permutabile e che un sottogruppo permutabile è modulare in G. Dunque un sottogruppo normale è sempre modulare in G.

Teorema 3.5.4. *Il reticolo dei sottogruppi normali di un gruppo qualsiasi e il reticolo dei sottogruppi di un gruppo abeliano sono modulari.*

Dimostrazione. Per il precedente teorema che ogni sottogruppo normale di un gruppo G è modulare in $L(G)$ e dunque anche nel reticolo dei sottogruppi normali, poiché esso è un sottoreticolo di $L(G)$. Dunque il reticolo dei sottogruppi normali è modulare e se G è abeliano, allora i due reticoli coincidono. □

Bibliografia

[1] Roland Schmidt, *Subgroup lattices of groups*, Walter de Gruyter, 1994

[2] Joseph J. Rotman, *An introduction to the theory of groups*, Springer-Verlag, 1994