ALGEBRA 1: TEOREMA DI LAGRANGE, OMOMORFISMI E GRUPPO QUOZIENTE

ALESSANDRO D'ANDREA

1. La nozione di gruppo

Iniziamo dalla definizione di gruppo:

Definizione 1.1. Un insieme G, dotato di un'operazione $\cdot : G \times G \to G$ si dice *gruppo* se

- l'operazione $\cdot$ è associativa;
- esiste in G un elemento e, detto "*identità*" , tale che $e \cdot g = g \cdot e = g$ per ogni $g \in G$;
- ogni elemento $g \in G$ ammette un "*inverso*" $g^{-1} \in G$, tale cioè che $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Scriverò spesso ab oppure $a \cdot b$ invece del più corretto $\cdot(a, b)$. Inoltre eviterò quasi sempre di scrivere parentesi per indicare l'ordine nel quale effettuare i prodotti. Questo è in effetti reso superfluo dall'associatività dell'operazione di gruppo. Richiedere che $(ab)c$ sia uguale ad $a(bc)$ basta ad assicurare che ogni possibile moltiplicazione di un numero qualsiasi di elementi dia lo stesso risultato, indipendentemente dall'ordine nel quale viene effettuato, a patto che si rispetti la posizione di ciascun fattore. Ad esempio, per il prodotto di quattro elementi, l'associatività comporta che:

$$a(b(cd)) = a((bc)d) = (a(bc))d = ((ab)c)d) = (ab)(cd),$$

il che mostra che trascurare le parentesi e scrivere $abcd$ non è solo un abuso di notazione, ma la conseguenza di un fenomeno naturale.

Di questo bisognerebbe dare una dimostrazione rigorosa. Farlo è semplice, ma letta la dimostrazione le idee potrebbero essere più confuse di prima.[1] Per avere un'idea di come mostrarlo, date un' occhiata al libro di Artin (la Proposizione 1.4) che vi ho consigliato.

Una notazione compatta per i prodotti aa, aaa, ecc... è di scrivere — come già si fa per il prodotto di numeri — a^2, a^3, ecc.... Con a^{-n} indicherò $(a^{-1})^n$. E' facile convincersi che $a^m a^n = a^{m+n}$ e che $(a^m)^n = a^{mn}$, se si pone $a^0 = e, a^1 = a$.

Esempi

(1) L'insieme S_X di tutte le applicazioni invertibili da un insieme X in se stesso, con l'operazione di composizione, è un gruppo, detto il *gruppo delle permutazioni di* X. Se X è un insieme finito, allora si sceglie solitamente $X = \{1, 2, ..., n\}$ e si scrive $\mathrm{S}_X = \mathrm{S}_n$. S_n ha $n!$ elementi.
(2) L'insieme delle rotazioni nel nel piano centrate nell'origine di angoli multipli di $2\pi/n$ è un gruppo, che si indica con C_n. Abbiamo visto che questo gruppo possiede n elementi, e che è un gruppo *ciclico*. Esso ammette cioè un elemento le cui potenze esauriscano tutti gli elementi del gruppo. Un elemento di tale tipo è detto *generatore* del gruppo ciclico. Ad esempio, la rotazione di $2\pi/n$ genera il gruppo ciclico C_n.
(3) L'insieme $\mathrm{GL}_n(\mathbf{k})$ delle matrici **non singolari** n per n a coefficienti in un campo $\mathbf{k}$ (ad esempio il campo $\mathbf{k} = \mathbb{R}$ dei numeri reali) è un gruppo rispetto al prodotto righe per colonne. Tale prodotto è infatti associativo, ed il prodotto di matrici di determinante non nullo è ancora una matrice di determinante non nullo. Inoltre l'identità ha determinante 1, ed ogni matrice non singolare si inverte con una matrice ancora non singolare.
(4) L'insieme $\mathrm{SL}_n(\mathbf{k})$ delle matrici n per n di determinante 1 è ancora un gruppo.
(5) Gli insiemi numerici $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, se considerati con l'operazione $+$ di **somma** sono gruppi. L'identità è l'elemento 0 mentre l'inverso di α è $-\alpha$.
(6) Se A è un anello con unità, $a \in A$ si dice *invertibile* se esiste un elemento $a^{-1} \in A$ tale che $aa^{-1} = a^{-1}a = 1$. L'insieme $A^\times$ degli elementi invertibili di A è un gruppo rispetto alla moltiplicazione. In effetti 1 è invertibile, e costituisce l'identità di $A^\times$, ed il prodotto ab di elementi invertibili $a, b \in A^\times$ è invertibile con inverso $b^{-1}a^{-1}$. $A^\times$ si indica talvolta con la notazione $U(A)$.

La notazione additiva nell'ultimo esempio non deve fuorviare: $+$ è decisamente un'operazione di gruppo. Indicare l'operazione di gruppo con $+$ invece che $\cdot$ è estremamente frequente quando l'operazione è commutativa, cioè quando $ab = ba$ per ogni coppia di elementi $a, b \in G$. Questi gruppi sono detti *abeliani*. Chiaramente, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sono abeliani. E' abeliano anche C_n, mentre non lo sono S_X, GL_n ed S_n.[2] Ora alcuni

Non-esempi

- La famiglia E_X di tutte le applicazioni dall'insieme X in se stesso non è un gruppo.[3] In effetti, la composizione è un'operazione associativa, e l'identità ne è l'elemento neutro. Però un'applicazione ha inversi sinistri

Date: 24 ottobre 2020.

[1] Ogni volta che si cerca di dimostrare un fatto intuitivo ed ovvio, si scopre che la dimostrazione non chiarisce nulla, oppure che il fatto era falso...
[2] A dire il vero, S_X è abeliano se X contiene meno di tre elementi, mentre GL_n ed SL_n sono abeliani se $n \leq 1$.
[3] ...a meno che X abbia meno di due elementi...

se e solo se è iniettiva, ed ha inversi destri se e solo se è suriettiva. Quindi non tutti gli elementi di E_X ammettono inverso.
- Se $n > 1$, l'insieme delle matrici n per n di determinante nullo non è un gruppo. Pur essendo il prodotto righe per colonne associativo, e il prodotto di matrici singolari ancora singolare, non esiste un elemento neutro per il prodotto.
- Gli insiemi di matrici $\mathrm{GL}_n(\mathbf{k}), \mathrm{SL}_N(\mathbf{k})$ non sono gruppi rispetto all'operazione di somma tra matrici.
- Gli insiemi $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ non sono gruppi se considerati rispetto all'operazione di prodotto. Infatti l'elemento 0 non ammette un inverso moltiplicativo. $\mathbb{Q} \setminus \{0\}$ e $\mathbb{R} \setminus \{0\}$ sono tuttavia gruppi rispetto al prodotto.

Una prima proprietà dei gruppi è la seguente:

Proposizione 1.2. *In un gruppo G esiste un'unica identità. Ogni elemento ammette un solo inverso. Inoltre $(g^{-1})^{-1} = g$, e $(gh)^{-1} = h^{-1}g^{-1}$.*

Dimostrazione. Siano e, e' elementi neutri per l'operazione di gruppo. Questo vuol dire che

$$ex = xe = e, \qquad e'x = xe' = x$$

per ogni scelta di $x \in G$. In particolare $e = ee' = e'$, e quindi vi è un solo elemento neutro.

La stessa cosa vale per l'inverso: se x e y sono entrambi inversi di g, allora $gx = xg = e, gy = yg = e$. Questo implica $x = xe = xgy = ey = y$, e quindi vi è un solo inverso di g. Le altre due proprietà seguono subito osservando che $gg^{-1} = g^{-1}g = e, ghh^{-1}g^{-1} = geg^{-1} = e$. □

Si vede che per invertire il prodotto gh bisogna moltiplicare gli inversi degli elementi g e h, **ma nell'ordine inverso**. Questo dipende dalla (possibile) non commutatività del prodotto. In un gruppo abeliano si avrebbe chiaramente $(ab)^{-1} = a^{-1}b^{-1}$. Bisogna stare attenti anche alle potenze di un prodotto: infatti $(ab)^3$ non è l'elemento a^3b^3, bensì $ababab$!!!

Definizione 1.3. Sia G un gruppo. Si dice che $g \in G$ ha *ordine infinito* se nessuna potenza positiva di g è uguale all'identità. Altrimenti, l'*ordine* di g è il minimo intero positivo n tale che $g^n = e$.

Ad esempio, l'identità ha sempre ordine 1, mentre ogni elemento non nullo di $\mathbb{Z}$ ha ordine infinito. L'ordine di g si indica con $o(g)$.

Proposizione 1.4. *Ogni elemento di un gruppo finito ha ordine finito.*

Dimostrazione. Le potenze di g — e cioè $g, g^2, g^3, g^4, ...$ — non possono essere tutte distinte, dal momento che il gruppo al quale appartengono ha un numero finito di elementi. Vi è quindi almeno una ripetizione, cioè possiamo trovare interi $m > n$ tali che $g^m = g^n$. Ma allora, moltiplicando per l'inverso di g^n, otteniamo $g^{m-n} = e$, e quindi g ha ordine finito. □

2. Sottogruppi

Definizione 2.1. Sia G un gruppo. Un sottoinsieme non vuoto $H \subset G$ si dice *sottogruppo* se H ammette una struttura di gruppo **rispetto allo stesso prodotto** di G.

Si vede facilmente, e lo abbiamo visto a lezione, che se $H < G$ allora le identità di H e di G coincidono, e l'inverso di un elemento in H è lo stesso che in G. Dal momento che l'operazione di gruppo di G ristretta ad H è automaticamente associativa, abbiamo

Proposizione 2.2. *Affinché un sottoinsieme non vuoto H sia un sottogruppo di G è sufficiente*[4] *che:*
- *se $a, b \in H$ allora anche $ab \in H$;*
- *se $a \in H$ allora anche $a^{-1} \in H$.*

Dimostrazione. L'identità e appartiene automaticamente ad H, che è pertanto non vuoto. Tutti gli altri assiomi di gruppo sono soddisfatti da H in quanto valgono per G. □

Il modo più semplice per verificare che un candidato sottogruppo sia non vuoto è ovviamente mostrare che contiene l'identità.

Corollario 2.3. *Affinché un sottoinsieme non vuoto* **e finito** *H sia sottogruppo di G è sufficiente che se $a, b \in H$ allora anche $ab \in H$.*

Dimostrazione. Sia H un sottoinsieme non vuoto di G che contiene il prodotto di due qualsiasi suoi elementi. H contiene allora tutte le potenze (ad esponente positivo) di ogni suo elemento.

Abbiamo già visto come ogni $a \in H$ abbia necessariamente ordine finito. Come conseguenza a^{-1} è una potenza positiva di a, quindi giace automaticamente in H. □

Esempi
(1) I sottoinsiemi $\{e\}$ e G sono sempre sottogruppi di G: sono detti *sottogruppi banali* di G.
(2) Sia $n \in \mathbb{Z}$. L'insieme (n) di tutti i multipli di n è un sottogruppo del gruppo additivo $\mathbb{Z}$.
(3) $\mathrm{SL}_n(\mathbf{k})$ è un sottogruppo di $\mathrm{GL}_n(\mathbf{k})$ per ogni campo $\mathbf{k}$.
(4) Sia $g \in G$. L'insieme di tutte le potenze positive e negative $(g) = \{g^i | i \in \mathbb{Z}\}$ è un sottogruppo di G detto *sottogruppo generato da g*. Il sottogruppo (g) è sempre abeliano.

[4] Nonché ovviamente necessario

3. Congruenze modulo un sottogruppo e classi laterali

Il concetto di congruenza modulo un sottogruppo generalizza quello di congruenza modulo n nel gruppo $\mathbb{Z}$ degli interi, e permette di mostrare il fondamentale teorema di Lagrange, che è punto di partenza per lo studio dei gruppi finiti.

Siano G un gruppo, e H un suo sottogruppo.

Definizione 3.1. Siano $a, b \in G$. Si dice che a è *congruo* a b modulo H, e si scrive

$$a \equiv b \mod H$$

se $a^{-1}b \in H$.

Teorema 3.2. *La congruenza modulo H è una relazione di equivalenza.*

Dimostrazione. Per mostrare la riflessività è sufficiente notare che $a \equiv a \mod H$ se e solo se $a^{-1}a = e \in H$. Ma questo è vero, poiché l'identità appartiene ad ogni sottogruppo di G. La simmetria si mostra in maniera simile: $a \equiv b \mod H$ se e solo se $a^{-1}b \in H$. Il suo inverso $b^{-1}a = (a^{-1}b)^{-1}$ è ancora un elemento di H, e quindi $b \equiv a \mod H$.

Anche la transitività è immediata: le congruenze $a \equiv b \mod H$, $b \equiv c \mod H$ sono equivalenti a $a^{-1}b, b^{-1}c \in H$. Ma H è un sottogruppo, e quindi il prodotto $a^{-1}c = (a^{-1}b)(b^{-1}c)$ è ancora un elemento di H, il che garantisce che $a \equiv c \mod H$. □

Nel caso della relazione di congruenza modulo un sottogruppo H, le classi di equivalenza sono facili da determinare. Abbiamo infatti mostrato a lezione che gli elementi congrui ad $a \in G$ modulo H sono tutti e soli quegli elementi di G che si scrivono come ah per qualche elemento $h \in H$.

Proposizione 3.3. *La classe di congruenza modulo H di $a \in G$ è il sottoinsieme $aH = \{ah | h \in H\}$.*

I sottoinsiemi del tipo aH si dicono *classi laterali sinistre*, o semplicemente *laterali sinistri*, di H in G. Avremmo potuto definire la relazione di congruenza modulo H anche tramite la condizione $ab^{-1} \in H$. Questa nuova condizione non è sempre equivalente all'altra che abbiamo dato, e fornisce in generale una relazione differente. Le sue classi di equivalenza sono date dai laterali destri Ha invece che da quelli sinistri. I sottogruppi per i quali i laterali sinistri coincidono con quelli destri, e quindi le due relazioni coincidono, si chiamano *sottogruppi normali*, e rivestono un ruolo importante nella teoria dei gruppi.

L'insieme quoziente di tutti i laterali sinistri di H in G si indica col simbolo G/H. L'insieme dei laterali destri viene invece indicato con $H\backslash G$: questa notazione è però molto rara, e viene utilizzata quasi esclusivamente quando si considerano *classi laterali doppie*.

4. Il Teorema di Lagrange e le sue conseguenze

La proprietà rilevante dei laterali sinistri di un sottogruppo H in un gruppo G è che hanno tutti la stessa cardinalità.

Proposizione 4.1. *L'applicazione $H \ni h \mapsto ah \in aH$ è una corrispondenza biunivoca.*

Dimostrazione. La suriettività segue dalla stessa definizione di aH. L'iniettività è facile: se $ah_1 = ah_2$, allora moltiplicando a sinistra per a^{-1} si ottiene $h_1 = h_2$. □

Definizione 4.2. L'*ordine* di un gruppo G è il numero dei suoi elementi, e si indica con $|G|$.

Lemma 4.3. *L'ordine di un elemento g di un gruppo G è uguale all'ordine del sottogruppo (g) di G generato da g.*

Dimostrazione. L'affermazione è evidente se l'ordine di g è infinito. In tal caso tutte le potenze positive di g sono distinte, ed il sottogruppo (g) ha quindi cardinalità infinita.

Se invece g ha ordine finito n, allora gli n elementi $e = g^0, g = g^1, \ldots, g^{n-1}$ sono tutti distinti. Inoltre ogni potenza di g è uguale ad uno di tali elementi: per la divisione euclidea tra gli interi, ogni $k \in \mathbb{Z}$ si può esprimere nella forma $k = qn + r$ con $0 \leq r < n$. Ma allora $g^k = g^{qn+r} = (g^n)^q g^r = g^r$. Abbiamo quindi mostrato che $(g) = \{e, g, \ldots, g^{n-1}\}$ possiede esattamente n elementi. □

Definizione 4.4. L'indice di H in G è il numero dei laterali sinistri di H in G (ovvero dell'insieme quoziente rispetto alla relazione di congruenza modulo H), e si indica con $[G : H]$.

La conclusione è immediata. G è un insieme che viene ripartito in laterali sinistri aH che hanno tutti la stessa cardinalità di H. Se il numero di laterali sinistri è $[G : H]$ allora si ha:

Teorema 4.5 (Lagrange)**.** *Se $H < G$ sono gruppi finiti, allora $|G| = |H|[G : H]$*

La notazione utilizzata per l'indice di H in G è suggestiva, infatti $[G : H] = |G|/|H|$. Il "diviso" non è solo un segno di interpunzione: è davvero, in qualche senso, un'operazione di divisione! Nel caso in cui G sia infinito, il Teorema di Lagrange continua ad essere valido interpretando $|H|[G : H]$ come prodotto di cardinalità.

Corollario 4.6. *Se H è un sottogruppo del gruppo finito G, allora l'ordine di H divide quello di G.*

Corollario 4.7. *Se g è un elemento del gruppo finito G, allora l'ordine di g divide quello di G. In particolare $g^{|G|} = e$.*

Dimostrazione. L'ordine dell'elemento g è pari a quello del sottogruppo $(g) = \{e, g, g^2, ..., g^{n-1}\}$ che genera in G. Pertanto, $|G| = o(g) \cdot [G : (g)]$, e di conseguenza

$$g^{|G|} = g^{o(g)\cdot[G:(g)]} = (g^{o(g)})^{[G:(g)]} = e^{[G:(g)]} = e.$$

□

Corollario 4.8. *Un gruppo di ordine primo è ciclico, e i suoi unici sottogruppi sono quelli banali.*

Dimostrazione. Sia $|G| = p$, con p primo. L'ordine degli elementi di G divide p, e può quindi essere uguale solo ad 1 oppure a p. L'identità è l'unico elemento che ha ordine 1, e tutti gli altri devono avere ordine p. Questo vuol dire che qualsiasi elemento $g \neq e$ è un generatore di G, e pertanto G è ciclico.

I sottogruppi sono necessariamente banali per lo stesso motivo: l'ordine di un sottogruppo è 1 oppure p, pertanto il sottogruppo contiene solo l'identità oppure tutti gli elementi del gruppo G. □

Abbiamo già visto che gli elementi invertibili di un anello costituiscono un gruppo rispetto all'operazione di moltiplicazione. Un caso notevole è quello del gruppo $(\mathbb{Z}/(n))^\times$ delle classi di resto invertibili modulo n. Sappiamo bene che una classe $\overline{a} \in \mathbb{Z}/(n)$ è invertibile se e solo se il massimo comun divisore $\mathrm{MCD}(a, n)$ è uguale ad 1. Il gruppo $U_n = (\mathbb{Z}/(n))^\times$ contiene $\phi(n)$ elementi.

Esempi: $U_p = \{1, 2, ..., p-1\}$ se p è primo.
$U_8 = \{1, 3, 5, 7\}$. $U_{10} = \{1, 3, 7, 9\}$. $U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$.

Il valore di $\phi(n)$ si calcola facilmente una volta nota la fattorizzazione di n. Si ha infatti:

$$\phi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Alternativamente, si può utilizzare il fatto che se m ed n sono primi tra loro, allora

$$\phi(mn) = \phi(m)\phi(n),$$

e che se p è primo, si ha:

$$\phi(p^n) = (p-1)p^{n-1}.$$

Teorema 4.9 (Eulero)**.** *Se a è primo con n, allora $a^{\phi(n)} \equiv 1 \mod n$.*

Dimostrazione. Il gruppo U_n ha ordine $\phi(n)$. Sia a primo con n, ed indichiamo con $\overline{a}$ la sua classe di resto modulo n. Allora, per il Lemma 4.7, $\overline{a}^{\phi(n)}$ è uguale all'identità di U_n, pertanto $a^{\phi(n)} \equiv 1 \mod n$. □

Questo teorema ha la semplice conseguenza:

Teorema 4.10 (Fermat)**.** *Se p è primo, allora $a^p \equiv a \mod p$.*

Dimostrazione. Sappiamo che $\phi(p) = p-1$. Se a è primo con p, allora $a^{p-1} \equiv 1 \mod p$. Moltiplicando per a si ottiene $a^p \equiv a \mod p$. Se invece a è divisibile per p, allora sia a^p che a sono congrui a 0 modulo p. □

4.1. **Qualche applicazione aritmetica del Teorema di Lagrange.**

Uno dei più celebrati teoremi di Euclide è il seguente:

Teorema 4.11. *Esistono infiniti numeri primi.*

Dimostrazione. L'enunciato dimostrato da Euclide è più precisamente il seguente: data una qualsiasi quantità finita di numeri primi, è possibile trovarne un altro. La dimostrazione è la seguente: se $p_1, \ldots, p_k$ sono numeri primi distinti, poniamo $N = p_1 \cdot \cdots \cdot p_k + 1 > 1$. Per il Teorema fondamentale dell'aritmetica, esiste almeno un primo q che divide N, e q è sicuramente diverso da ciascun p_1, poiché N non è loro multiplo. □

Non è difficile adattare questo ragionamento a enunciati più raffinati.

Teorema 4.12. *Esistono infiniti numeri primi della forma $4n - 1$.*

Dimostrazione. Siano $p_1 = 3, p_2, \ldots, p_k$ numeri primi $\equiv 3 \mod 4$ e poniamo $N = 4p_1 \cdot \cdots \cdot p_k - 1 > 1$ in modo che $N \equiv 3 \mod 4$. Poiché N è dispari, è diviso solo da primi dispari. Ma tali primi non possono essere tutti $\equiv 1 \mod 4$, perché altrimenti il loro prodotto N sarebbe $\equiv 1 \mod 4$. Pertanto almeno uno dei primi che dividono N è $\equiv 3 \mod 4$, e deve essere diverso da $p_1, \ldots, p_k$ che non dividono N. □

Per esercizio adattate l'argomento appena visto per mostrare che esistono infiniti primi della forma $6n - 1$. Il Teorema di Lagrange può essere utilizzato, in modo un po' diagonale, per dimostrare che anche l'altra classe di resto invertibile modulo 4 e 6 contiene infiniti numeri primi. Vediamo come:

Teorema 4.13. *Esistono infiniti numeri primi della forma $4n + 1$.*

Dimostrazione. Siano $p_1, \dots, p_k$ primi congrui a 1 modulo 4, e poniamo $N = 2p_1 \cdot \dots \cdot p_k$. Sia q un primo che divide $N^2 + 1$; chiaramente q è un primo dispari diverso da ciascun p_i.

Abbiamo $N^2 \equiv -1 \mod q$ e poiché $q > 2$, $-1 \not\equiv 1 \mod q$. Poiché $N^4 = (N^2)^2 \equiv (-1)^2 = 1 \mod q$, la classe di resto $[N] \in \mathbb{Z}/(q)^\times$ ha ordine che divide 4 ma non divide 2 – in altre parole, l'ordine moltiplicativo di $[N]$ in $\mathbb{Z}/(q)^\times$ è esattamente 4. Per il Teorema di Lagrange, 4 divide allora $|\mathbb{Z}/(q)^\times| = q - 1$ e quindi $q \equiv 1 \mod 4$. Abbiamo quindi mostrato che data qualsiasi quantità di primi $\equiv 1 \mod 4$ è possibile trovarne almeno un altro. □

Teorema 4.14. *Esistono infiniti numeri primi della forma* $6n + 1$.

Dimostrazione. Siano $p_1, \dots, p_k$ primi congrui a 1 modulo 6, e poniamo $N = 6p_1 \cdot \dots \cdot p_k$. Sia q un primo che divide $N^2 - N + 1$; chiaramente $q \neq 2, 3$ è un primo dispari diverso da ciascun p_i.

Poiché $N^3 + 1 = (N + 1)(N^2 - N + 1)$, abbiamo $N^3 \equiv -1 \mod q$ e poiché $q > 2$, $-1 \not\equiv 1 \mod q$. Come prima $N^6 = (N^3)^2 \equiv (-1)^2 = 1 \mod q$, e la classe di resto $[N] \in \mathbb{Z}/(q)^\times$ ha quindi ordine che divide 6 ma non divide 3 – in altre parole, l'ordine moltiplicativo di $[N]$ in $\mathbb{Z}/(q)^\times$ è 6 oppure 2.

E' comunque possibile escludere l'eventualità che $[N]$ abbia ordine 2: dire che $N^2 \equiv 1 \mod q$ significa che q divide $N^2 - 1$. Ma allora q divide $(N^2 - 1) - (N^2 - N + 1) = N - 2$ e anche $(N^2 - 1) - (N + 2)(N - 2) = 3$. Sappiamo già che $q \neq 3$ e questo è quindi un assurdo.

In conclusione, l'ordine di $[N]$ nel gruppo moltiplicativo $\mathbb{Z}/(q)^\times$ è 6 e il Teorema di Lagrange ci assicura che 6 divide $q - 1$. Concludiamo che $q \equiv 1 \mod 4$ e che data qualsiasi quantità di primi $\equiv 1 \mod 6$ è possibile trovarne almeno un altro. □

5. Intersezione e prodotto di sottogruppi

Studiando l'algebra lineare, abbiamo già visto che l'intersezione di sottospazi vettoriali è un sottospazio vettoriale. Per ottenere il sottospazio generato da due sottospazi vettoriali non era invece sufficiente prendere l'unione dei due sottospazi, ma piuttosto la *somma* dei due, ovvero l'insieme di tutte le somme di un elemento del primo sottospazio con un elemento del secondo.

La situazione, nel caso dei gruppi abeliani, è praticamente la stessa. Per quanto riguarda quelli non abeliani bisogna prestare invece un po' di attenzione. La proposizione che segue non è stata menzionata a lezione, ma è di facile dimostrazione.

Proposizione 5.1. *L'intersezione $H \cap K$ di due sottogruppi $H, K < G$ è un sottogruppo di G.*

Dimostrazione. $H \cap K$ è non vuoto, dal momento che l'identità e vi appartiene sicuramente. Per mostrare che se $a, b \in H \cap K$ allora $ab \in H \cap K$ basta notare che a e b appartengono entrambi sia ad H che a K. Essendo questi insiemi sottogruppi, sono chiusi rispetto al prodotto, perciò ab giace sia in H che in K, quindi nella loro intersezione. Per quanto riguarda l'inverso, il ragionamento è del tutto analogo. □

Proposizione 5.2. *Il prodotto $HK = \{hk | h \in H, k \in K\}$ di sottogruppi di G è un sottogruppo se e solo se $HK = KH$.*

Dimostrazione. Se HK è un sottogruppo di G, allora deve contenere $kh = (h^{-1}k^{-1})^{-1} \in HK$ per ogni $h \in H, k \in K$, e quindi $KH \subset HK$. Inoltre, se $x \in HK$, allora anche $x^{-1} \in HK$; se $x^{-1} = hk$, allora $x = k^{-1}h^{-1} \in KH$, il che mostra che anche $HK \subset KH$, e quindi $HK = KH$.

Il viceversa è più facile: se $HK = KH$, è immediato vedere che il prodotto di elementi di HK giace ancora in HK, e lo stesso è vero per l'inverso di ogni elemento. □

Utilizzeremo sporadicamente il seguente risultato:

Proposizione 5.3. *Il sottoinsieme HK ha esattamente $|H||K|/|H \cap K|$ elementi.*

Dimostrazione. Quando succede che $hk = h'k'$ se $h, h' \in H$ e $k, k' \in K$? $hk = h'k'$ è equivalente a $h'^{-1}h = k'k^{-1}$: il primo membro appartiene ad H mentre il secondo a K, quindi $d = h'^{-1}h = k'k^{-1}$ appartiene all'intersezione $H \cap K$. Ricapitolando, se $hk = h'k'$, allora $k' = (k'k^{-1})k = dk$, mentre $h' = h(h^{-1}h') = h(h'^{-1}h)^{-1} = hd^{-1}$. Viceversa, i prodotti hk e $(hd^{-1})(dk)$ forniscono lo stesso risultato per ogni $d \in H \cap K$.

Concludendo, ci sono $|H||K|$ possibili modi di moltiplicare un elemento di H per un elemento di K, ma ogni risultato hk viene ottenuto $|H \cap K|$ volte distinte: una per ogni scelta di $d \in H \cap K$. I risultati ottenuti sono quindi $|H||K|/|H \cap K|$, e questa è esattamente la cardinalità dell'insieme HK. □

Corollario 5.4. *Se G è abeliano, e $H, K < G$, allora HK è sempre un sottogruppo.*

Un'osservazione ovvia, ma utile, prima di concludere. Nel caso si stia utilizzando la notazione additiva all'interno di un gruppo, si scriverà ovviamente $H + K$ invece di HK.

6. Esempi

6.1. **Il gruppo $\mathbb{Z}$.** L'insieme $\mathbb{Z}$, con l'operazione $+$ di somma, costituisce un gruppo abeliano. Infatti, $+$ è un'operazione commutativa ed associativa, della quale 0 è l'elemento neutro. L'inverso (additivo) dell'elemento n è $-n$, pertanto ogni elemento ammette inverso. $\mathbb{Z}$ è un gruppo ciclico; i suoi due generatori ciclici sono 1 e -1.

Chiaramente il sottoinsieme (n) di $\mathbb{Z}$ composto dai multipli di un intero n fissato è un sottogruppo (ancora ciclico) di $\mathbb{Z}$. A lezione abbiamo mostrato:

Teorema 6.1. *I sottogruppi di $\mathbb{Z}$ sono tutti della forma (n) per qualche $n \in \mathbb{N}$.*

Dimostrazione. L'argomento che abbiamo utilizzato per dimostrare che gli ideali di $\mathbb{Z}$ sono tutti principali funziona anche in questo caso *senza cambiare una virgola*. Sia H un sottogruppo di $\mathbb{Z}$: se contiene solo lo 0, allora $H = (0)$ ed abbiamo concluso. Se invece H non contiene solo lo (0) contiene certamente elementi positivi. Sia n il minimo elemento positivo di H.

Allora $H = (n)$. Infatti, H contiene certamente tutti i multipli di n. Inoltre, H non può contenere un elemento a non multiplo di n. Dovrebbe infatti contenere anche il resto della divisione euclidea di a per n: un intero positivo minore di n. Questo fatto è una contraddizione con l'ipotesi che n fosse il minimo elemento di H. □

La relazione di congruenza modulo il sottogruppo (n) è la normale congruenza modulo n tra gli interi.

Proposizione 6.2. *Siano m e d il minimo comune multiplo ed il massimo comun divisore degli interi a ed b. Allora $(a) \cap (b) = (m), (a) + (b) = (d)$.*

Dimostrazione. $(a) \cap (b)$ è sicuramente un sottogruppo, i cui elementi sono multipli sia di a che di b. Il suo minimo elemento positivo è pertanto m, da cui $(a) \cap (b) = (m)$. Anche $(a) + (b)$ è un sottogruppo, pertanto della forma $(d), d \geq 0$. Gli interi a e b appartengono a (d), pertanto d è un divisore comune di a e b.

Per mostrare che d è il massimo tra i divisori comuni di a e b, notiamo dapprima che $d \in (a) + (b)$, e che quindi si può scrivere come somma di un multiplo di a e di uno di b. In altre parole esistono interi h, k tali che $d = ha + kb$. Se $d' \geq 0$ è un divisore comune di a e b, allora deve dividere anche $d = ha + kb$, e pertanto $d' \leq d$. In altre parole, d è il più grande tra i divisori comuni di a e b. □

6.2. **Gruppi ciclici e diedrali.** Le isometrie del piano formano gruppo rispetto all'operazione di composizione. Infatti, la composizione di isometrie è chiaramente un'isometria; inoltre, l'identità è isometrica, e l'inverso di ogni isometria è ovviamente ancora una isometria.

Vi sono due tipi di isometrie: quelle che conservano l'orientazione e quelle che la invertono. Un semplice teorema di algebra lineare ci informa che le isometrie del piano che conservano l'orientazione sono traslazioni e rotazioni, mentre quelle che la invertono sono delle simmetrie rispetto ad una retta.

Fissiamo un n-agono regolare nel piano, e chiamiamo D_n (rispettivamente C_n) l'insieme delle isometrie (risp. isometrie che conservano l'orientazione) che lo conservano, cioè che lo sovrappongono esattamente a se stesso. D_n e C_n contengono l'identità, e sono quindi insiemi non vuoti. Il gruppo C_n è generato dalla rotazione di $2\pi/n$ attorno al centro dell'n-agono, ed è quindi ciclico di ordine n. Il gruppo D_n si chiama *gruppo diedrale*, e contiene strettamente C_n come sottogruppo.

Proposizione 6.3. $|\mathrm{D}_n| = 2n$.

Dimostrazione. Ogni elemento di D_n è univocamente determinato dalla scelta delle immagini di due suoi vertici consecutivi. Le possibili immagini sono le coppie ordinate di vertici consecutivi dell'n-agono, che sono appunto $2n$. Questo mostra, in particolare, che D_n contiene n rotazioni ed n simmetrie. □

Sia ora ρ la rotazione in senso antiorario di $2\pi/n$, e scegliamo una simmetria $s \in \mathrm{D}_n$. Le potenze $\rho^i, 0 \leq i < n$ esauriscono le n rotazioni contenute in D_n. Inoltre $sx = sy$ se e solo se $x = y$ (basta moltiplicare a sinistra per $s^{-1} = s$). Pertanto gli elementi $s\rho^i, 0 \leq i < n$ sono n elementi distinti di D_n, e nessuno tra essi può essere una rotazione, perché rovescia l'orientazione del piano. Abbiamo così dimostrato la

Proposizione 6.4. *Gli elementi $\rho^i, s\rho^i$, dove $i = 0, 1, ..., n-1$, formano un elenco completo di elementi distinti di D_n.*

In particolare tutti gli elementi $\rho^i s$ sono simmetrie, dal momento che gli elementi ρ^i esauriscono tutte le rotazioni di D_n. L'operazione di gruppo in D_n si descrive in modo semplice.

Lemma 6.5. *$\rho^i s = s\rho^{-i}$ per ogni $n \in \mathbb{Z}$.*

Dimostrazione. L'elemento $s\rho^i$ è una simmetria, ed ha perciò ordine 2. Questo mostra che $s\rho^i s\rho^i = e$, da cui si ottiene l'enunciato moltiplicando per ρ^{-i} a destra, e per s a sinistra. □

Proposizione 6.6. *La composizione in D_n è tale che*

$$\rho^i \cdot \rho^j = \rho^{i+j}, \qquad s\rho^i \cdot \rho^j = s\rho^{i+j}$$
$$\rho^i \cdot s\rho^j = s\rho^{j-i}, \qquad s\rho^i \cdot s\rho^j = \rho^{j-i}$$

dove l'esponente di ρ si intende sempre modulo n.

E' facile determinare tutti i sottogruppi di C_n e D_n.

Proposizione 6.7. *I sottogruppi di C_n sono tutti ciclici, e precisamente della forma $\mathrm{C}_m = (\rho^d)$, dove d è un divisore di n, e $n = md$.*

Dimostrazione. Sia H un sottogruppo di $\mathrm{C}_n = (\rho)$. Definiamo $E = \{m \in \mathbb{N} | \rho^m \in H\}$. Chiaramente, $n \in E$. Inoltre E è un sottogruppo di $\mathbb{Z}$, quindi è del tipo (d), per qualche $d \in \mathbb{N}$. Dal momento che $n \in E = (d)$, allora d divide n, ed $H = (\rho^d)$. □

Vale la pena di notare che (ρ^n) è semplicemente (e).

Proposizione 6.8. *Gli unici sottogruppi di D_n sono i sottogruppi ciclici C_m e quelli diedrali della forma $\langle \mathrm{C}_m, s \rangle$ dove m è un divisore di n e $s \notin \mathrm{C}_n$.*

Dimostrazione. Sia H un sottogruppo di D_n. Vi sono due possibilità: H è completamente contenuto in $\mathrm{C}_n < \mathrm{D}_n$, oppure vi è qualche elemento di H che inverte l'orientazione del piano. Nel primo caso, H è un sottogruppo di C_n, ed è quindi della forma C_m per la Proposizione 6.7.

Nel secondo caso, H contiene il sottogruppo $K = H \cap \mathrm{C}_n$, che è C_m per un divisore opportuno m di n. Consideriamo in H la relazione di congruenza modulo K. Vi sono soltanto due classi di equivalenza: quella delle rotazioni e quella delle simmetrie. Infatti, se $a, b \in H$ conservano entrambe, o invertono entrambe, l'orientazione, allora $a^{-1}b \in H$ conserva l'orientazione, ed è perciò una rotazione contenuta in K. Se invece una sola tra a e b è una rotazione, allora $a^{-1}b$ è una simmetria, e pertanto non contenuta in K. Questo mostra che K ha indice 2 in H, e quindi H contiene $2n$ elementi. Di conseguenza H è generato da C_m insieme ad una qualsiasi simmetria $s \in H$. □

6.3. **Gruppi di ordine piccolo.** Darò ora la classificazione di tutti i gruppi di ordine minore di 8. **Non abbiamo fatto queste cose a lezione**, ma costituiscono un buon esercizio.

In realtà descriverò, più che i gruppi stessi, le classi di isomorfismo; il problema è che il concetto di isomorfismo tra gruppi sarà introdotto più avanti in questi appunti. Ci accontenteremo di una definizione intuitiva di questo concetto: per il momento, due gruppi *sono lo stesso gruppo* se le uniche differenze tra i due gruppi sono i nomi degli elementi. Ad esempio, il gruppo ciclico C_n ed il gruppo delle classi di resto modulo n sono chiaramente "lo stesso gruppo" . Voi state leggendo queste note dopo che il corso si è già concluso, quindi il concetto di gruppi isomorfi vi è comunque chiaro.

Andiamo "per ordine": se $|G| = 1$, allora $G = (e)$ e non c'è altro da dire. Se l'ordine p di G è un numero primo, abbiamo già visto come G sia necessariamente ciclico, e quindi $G = \mathrm{C}_p$. Questo risolve i casi $|G| = 2, 3, 5, 7$. Gli unici casi interessanti da trattare sono quindi $|G| = 4$ oppure 6.

6.3.1. *Gruppi di ordine* 4. Il teorema di Lagrange, che è per il momento lo strumento più sofisticato che abbiamo, ci dice che l'ordine degli elementi di un gruppo divide l'ordine del gruppo stesso. Se $|G| = 4$, allora, l'ordine degli elementi deve essere $1, 2$ oppure 4. Se G contiene un elemento di ordine 4, allora è ciclico, ed è C_4. Se G non contiene elementi di ordine 4, allora tutti gli elementi oltre l'identità devono avere ordine 2.

Facciamo un elenco degli elementi. Oltre all'identità avremo tre elementi a, b, c. Ognuno di questi elementi ha ordine 2, e pertanto è uguale al suo inverso. Quanto fa ab? Vediamo: il risultato non può essere a, perché $ab = a$ implica $b = e$. Per lo stesso motivo non può essere b. ab non può neanche essere l'identità, dal momento che $ab = e$ avrebbe come conseguenza $b = a^{-1} = a$. L'unica possibilità è che sia $ab = c$. Questo ragionamento si applica a qualsiasi prodotto di due tra gli elementi $a, b, c,$. Avremo quindi $ab = ba = c$, $ac = ca = b$, $bc = cb = a$. Questo è l'unico altro gruppo di ordine 4. E' abeliano, e talvolta si chiama V_4. Vedremo più in là una ricetta per dare un nome ad ogni gruppo abeliano. Il nome che questo gruppo avrà, per il momento misterioso, è $\mathrm{C}_2 \times \mathrm{C}_2$.

6.3.2. *Gruppi di ordine* 6. Usiamo sempre il teorema di Lagrange: i nostri elementi possono avere ordine $1, 2, 3$ oppure 6. Se G contiene un elemento di ordine 6 allora è il gruppo ciclico C_6. Se non contiene elementi di ordine 6, allora oltre all'identità ci sono solo elementi di ordine 2 o 3. Abbiamo tre casi:

(1) **Gli elementi diversi dall'identità hanno tutti ordine 2.** In questo caso, scelti due di questi elementi $a \neq b$, l'insieme $\{e, a, b, ab\}$ forma un sottogruppo (perché?) di ordine 4. Ma 4 non divide 6, e questo ci fornisce una contraddizione. Non esistono quindi gruppi di ordine 6 di questo tipo.

(2) **Gli elementi diversi dall'identità hanno tutti ordine 3.** Gli elementi di ordine 3 si raggruppano tutti a coppie di elementi inversi tra loro: $a, a^{-1} = a^2$. In G abbiamo pertanto l'identità, e poi coppie di elementi di ordine 3: in totale un numero dispari di elementi. Ma l'ordine di G è 6, che non è dispari. Anche questo caso non è quindi possibile.

(3) **Ci sono sia elementi di ordine 2 che di ordine 3.** Sia a un elemento di ordine 3, e b uno di ordine 2. Se $H = (a)$ e $K = (b)$, allora $H \cap K = (e)$, e quindi HK ha 6 elementi, così come KH. Questo mostra che $HK = KH = G$. Se

$$H = \{e, a, a^2\}, \qquad K = \{e, b\},$$

allora

$$HK = \{e, a, a^2, b, ab, a^2b\}, \qquad KH = \{e, a, a^2, b, ba, ba^2\}.$$

Questi due elenchi di elementi coincidono per quanto riguarda e, a, a^2 e b. Gli altri due elementi sono ab, a^2b in un caso e ba, ba^2 nell'altro. Pertanto, o $ab = ba$, oppure $ab = ba^2 = ba^{-1}$. Il secondo caso ci dà il gruppo diedrale, ovvero S_3, mentre il primo caso non è possibile! Infatti, qual è l'ordine di ab? Poiché $ab = ba$, G è un gruppo abeliano. Allora $(ab)^2 = a^2b^2 = a^2, (ab)^3 = a^3b^3 = b$. Questo vuol dire che ab non ha ordine né 2 né 3. Ha allora ordine 6, un assurdo col fatto di aver supposto che G non contenesse elementi di tale ordine.

Ricapitolando:

- $|G| = 1 : G = (e)$
- $|G| = 2 : G = \mathrm{C}_2$
- $|G| = 3 : G = \mathrm{C}_3$
- $|G| = 4 : G = \mathrm{C}_4$ opp. V_4
- $|G| = 5 : G = \mathrm{C}_5$
- $|G| = 6 : G = \mathrm{C}_6$ opp. $\mathrm{S}_3 = \mathrm{D}_3$
- $|G| = 7 : G = \mathrm{C}_7$

è la lista dei gruppi di ordine < 8, a meno di isomorfismo. Di questi solo S_3 è non abeliano.

Esercizio (per il momento difficile!): Trovate tutti i gruppi **non abeliani** di ordine 8 — ovviamente, a meno di isomorfismo!

Prima di passare ad altro, un'osservazione. Nella classificazione dei gruppi di ordine 6 abbiamo dimostrato, senza evidenziare particolarmente il fatto, questo risultato.

Teorema 6.9. *Se $|G|$ è pari, allora G contiene un elemento di ordine 2.*

Dimostrazione. Raccogliamo ogni elemento g assieme al proprio inverso g^{-1}. Gli unici elementi che stiano da soli sono gli elementi uguali al proprio inverso, ovvero l'identità e gli elementi di ordine 2.

Se G non contiene elementi di ordine 2, l'unico elemento a presentarsi singolarmente è l'identità, mentre gli altri vengono a coppie. In altre parole, G conterrebbe un numero dispari di elementi. Dal momento che $|G|$ è pari, vi sono necessariamente elementi di ordine 2 (ed in totale sono in numero dispari!!!!) □

Vedremo fra non molto un teorema di Cauchy che generalizza questo risultato:

Teorema 6.10 (Cauchy)**.** *Se un numero primo p divide $|G|$, allora G contiene un elemento di ordine p.*

6.4. **Gruppi simmetrici.** Senza troppi fronzoli, richiamo le cose che abbiamo scoperto. Una permutazione di un insieme X è una applicazione $\sigma : X \to X$ iniettiva e suriettiva, cioè invertibile. L'insieme S_X delle permutazioni di X è un gruppo rispetto all'operazione di composizione.

Per individuare una permutazione bisogna descriverla in qualche maniera. La maggior parte delle volte, X sarà un insieme finito, ed indicheremo i suoi elementi con i numeri da 1 ad n. S_X si indica in questo caso con S_n. Quando siamo in questa situazione, una permutazione si può descrivere come segue:

$$\sigma : \begin{cases} 1 \to 2 \\ 2 \to 1 \\ 3 \to 3 \end{cases}$$

che indica la permutazione tale che $\sigma(1) = 2, \sigma(2) = 1, \sigma(3) = 3$.

Abbiamo visto a lezione una notazione più compatta, che abbiamo chiamato *decomposizione di una permutazione in prodotto di cicli disgiunti*. Un numero finito di elementi sono *permutati ciclicamente* se ognuno viene mandato nel successivo, e l'ultimo nel primo. Una permutazione è un *ciclo*[5], o più precisamente un n-ciclo, se si possono trovare n elementi che vengono permutati ciclicamente, mentre gli altri vengono mandati in se stessi. Un 2-ciclo si dice anche *trasposizione*. Per individuare una permutazione ciclica è sufficiente elencare gli n elementi che vengono permutati ciclicamente nell'ordine in cui ognuno va nel successivo. Ad esempio il 4-ciclo

$$\tau : \begin{cases} 1 \to 5 \\ 2 \to 3 \\ 3 \to 1 \\ 4 \to 4 \\ 5 \to 2 \end{cases}$$

può essere più semplicemente indicato con (1523), che illustra come $\tau(1) = 5, \tau(5) = 2, \tau(2) = 3, \tau(3) = 1$. Questa notazione non è unica: $(5231), (2315), (3152)$ descrivono la stessa permutazione. Diventa però univocamente determinata se decidiamo di scrivere il ciclo a partire dal suo elemento minore.

La notazione compatta per indicare una permutazione qualsiasi consiste nello scrivere esplicitamente tutti i suoi cicli, trascurando gli elementi che vengono invece mandati in se stessi. Ad esempio le due permutazioni di S_7:

$$\phi : \begin{cases} 1 \to 2 \\ 2 \to 5 \\ 3 \to 7 \\ 4 \to 1 \\ 5 \to 4 \\ 6 \to 3 \\ 7 \to 6 \end{cases} \qquad \psi : \begin{cases} 1 \to 6 \\ 2 \to 4 \\ 3 \to 2 \\ 4 \to 5 \\ 5 \to 1 \\ 6 \to 7 \\ 7 \to 3 \end{cases}$$

si scriveranno $\phi = (1254)(376)$ e $\psi = (1673245)$, mentre $\phi\psi = (1352)$ e $\psi\phi = (1462)$ L'ordine di un ciclo è pari alla sua lunghezza. Pertanto l'ordine di un n-ciclo è n. L'ordine di un prodotto di cicli disgiunti è invece il minimo comune multiplo delle lunghezze dei suoi cicli.

Il gruppo S_n ha $n!$ elementi. I 6 elementi di S_3 sono ad esempio: $e, (12), (13), (23), (123), (132)$.

Le permutazioni si distinguono in *pari* e *dispari*. Consideriamo il prodotto $\prod_{i>j}(i-j)$. Se agiamo con una permutazione σ sui numeri $1, ..., n$, otteniamo

$$\prod_{i>j} (\sigma(i) - \sigma(j)) .$$

[5]Chiameremo i cicli anche *permutazioni cicliche*

E' facile convincersi che i fattori che compaiono in questo secondo prodotto siano gli stessi di prima, **a parte il segno**. La permutazione si dice pari se il risultato di questo prodotto è lo stesso di $\prod_{i>j}(i-j)$, ed è dispari se invece, complessivamente, cambia segno.

Ad esempio, in S_3, $(2-1)(3-1)(3-2)=2$. Alla permutazione (12) corrisponde il prodotto $(1-2)(3-2)(3-1)=-2$ mentre alla permutazione (123) corrisponde $(3-2)(1-2)(1-3)=2$. Perciò, la permutazione (12) è dispari, mentre (123) è pari. Dovrebbe essere più o meno evidente che la parità del prodotto di permutazioni segue le stesse regole del prodotto dei segni: permutazioni con la stessa parità hanno prodotto pari, mentre permutazioni con parità opposta hanno prodotto dispari. Ogni trasposizione è dispari, mentre un n-ciclo è pari se n è dispari, e dispari se n è pari.

L'insieme di tutte le permutazioni pari è chiaramente un sottogruppo, detto *sottogruppo alterno* di S_n, e si indica con A_n.

Proposizione 6.11. *A_n ha indice 2 in S_n. Se H è un sottogruppo di S_n non interamente contenuto in A_n, allora $H\cap\mathrm{A}_n$ ha indice 2 in H.*

Dimostrazione. Due permutazioni σ e τ sono congrue modulo A_n quando $\sigma\tau^{-1}$ è pari, cioè quando hanno la stessa parità. Vi sono quindi solo due classi laterali destre di A_n, che ha pertanto indice 2 e ordine $n!/2$. Lo stesso discorso vale per un sottogruppo H di S_n non contenuto in A_n. □

Come esercizio, elenchiamo tutti i sottogruppi di S_4. L'ordine dei sottogruppi di S_4 divide $4!=24$. I divisori di 24 sono $1,2,3,4,6,8,12$ e 24. Sia $H<\mathrm{S}_4$: se $|H|=1$ o 24 allora H è un sottogruppo banale. I sottogruppi ciclici sono facili da determinare: sono generati da singoli elementi di S_4. Le trasposizioni e i prodotti di due trasposizioni disgiunte generano sottogruppi ciclici di ordine 2, i 3-cicli ne generano di ordine 3, e i 4-cicli di ordine 4. D'altronde, i sottogruppi di ordine 2 e 3 devono essere necessariamente ciclici, pertanto se H non è ciclico, possiamo limitarci a studiare i casi $|H|=4,6,8,12$.

Prima di procedere, due osservazioni utili:

Lemma 6.12. *Il sottogruppo alterno A_4 contiene l'identità, i tre prodotti di due trasposizioni disgiunte, e gli otto 3-cicli.*

Lemma 6.13. *A_4 non ha sottogruppi di ordine 6.*

Dimostrazione. Non vi sono elementi di ordine 6, quindi A_4 non ha sottogruppi ciclici di ordine 6. Abbiamo appena visto che un gruppo non ciclico di ordine 6 possiede due elementi di ordine 3 e tre di ordine 2. In particolare, se un sottogruppo di A_4 ha ordine 6 deve contenere i tre elementi di ordine 2 che A_4 contiene, e quindi ammettere il sottogruppo[6] $\{e,(12)(34),(13)(24),(14)(23)\}$. Ma questo è assurdo, dal momento che 4 non divide 6. □

In ciò che segue, H è un sottogruppo non ciclico di S_4.

$|\mathbf{H}|=\mathbf{4}$. Se H è interamente contenuto in A_4, allora H può contenere solo gli elementi e, $(12)(34)$, $(13)(24)$ e $(14)(23)$, che sono gli unici ad avere ordine che divide 4. Si controlla facilmente che tali elementi formano effettivamente un sottogruppo.

Se invece H non è contenuto in A_4, allora $H\cap\mathrm{A}_4$ possiede due elementi, e quindi contiene solo un prodotto di due trasposizioni disgiunte. Gli altri elementi di H devono essere permutazioni dispari, che hanno ordine 2 essendo H non ciclico. Facciamo un esempio pratico: se $H\cap\mathrm{A}_4=\{e,(12)(34)\}$, H può contenere solo (12) e (34) perché il prodotto di $(12)(34)$ con le altre permutazioni fornisce come risultato 4-cicli. Ricapitolando, i quattro sottogruppi non ciclici di ordine 4 sono quindi

$$\{e,(12)(34),(13)(24),(14)(23)\},\qquad \{e,(12),(34),(12)(34)\},$$
$$\{e,(13),(24),(13)(24)\},\qquad \{e,(14),(23),(14)(23)\}.$$

$|\mathbf{H}|=\mathbf{6}$. H non è ciclico ed ha quindi tre elementi di ordine 2 e due di ordine 3. Questi ultimi sono 3-cicli, e sono elementi pari. Abbiamo visto che H non è contenuto in A_4, e quindi gli elementi di ordine due devono essere dispari, e perciò trasposizioni. Queste non possono fissare l'elemento fissato dai 3-cicli, perché altrimenti potremmo ottenere un 4-ciclo come prodotto di tale trasposizione per il 3-ciclo (ad esempio: $(123)(34)=(1234)$), e 4 non divide $|H|$. Perciò le trasposizioni muovono gli elementi che sono permutati dai 3-cicli. Questo ci fornisce 4 sottogruppi:

$$\{e,(12),(13),(23),(123),(132)\},\qquad \{e,(12),(14),(24),(124),(142)\},$$
$$\{e,(13),(14),(34),(134),(143)\},\qquad \{e,(23),(24),(34),(234),(243)\}.$$

$|\mathbf{H}|=\mathbf{8}$. H non è contenuto in A_4, poiché 8 non divide 12, quindi il sottogruppo degli elementi pari di H è $\{e,(12)(34),(13)(24),(14)(23)\}$. Gli elementi dispari che H può contenere sono trasposizioni o 4-cicli. In ogni caso, moltiplicando una trasposizione per uno dei tre prodotti di due trasposizioni si ottiene un 4-ciclo, e quindi H contiene necessariamente un 4-ciclo. Alla stessa maniera se H contiene un 4-ciclo, contiene anche una trasposizione — basta moltiplicare il 4-ciclo per uno, tra gli elementi $(12)(34),(13)(24),(14)(23)$ che non sia il suo quadrato. I possibili sottogruppi di otto elementi sono quindi determinati:

$$\{e,(12),(34),(12)(34),(13)(24),(14)(23),(1324),(1423)\},$$
$$\{e,(13),(24),(12)(34),(13)(24),(14)(23),(1234),(1432)\},$$
$$\{e,(14),(23),(12)(34),(13)(24),(14)(23),(1243),(1342)\}.$$

[6] Verificate che lo sia!!!

$|\mathbf{H}| = \mathbf{12}$. Se H è contenuto in A_4, coincide con esso. Se H non è contenuto in A_4, allora $H \cap \mathrm{A}_4$ ha ordine 6. Ma abbiamo già visto che A_4 non ha sottogruppi di ordine 6.

Esercizi:

(a) Sia G un gruppo **abeliano**, ed a, b elementi di G di ordine m ed n rispettivamente. Che si può dire dell'ordine di ab?

(b) Dare esempi di gruppi in cui il prodotto di elementi di ordine 2 abbia ordine $1, 2, 3$.

(c) Sull'insieme $\mathbb{Z}$ definiamo il prodotto

$$a \circ b = \begin{cases} a + b \text{ se } a \text{ è pari} \\ a - b \text{ se } a \text{ è dispari} \end{cases}$$

Fate vedere che $\mathbb{Z}$ è un gruppo rispetto all'operazione $\circ$, e che contiene elementi di ordine 2 il cui prodotto ha ordine infinito. Mostrate inoltre che $(\mathbb{Z}, \circ)$ ammette un sottogruppo infinito di indice 2.

7. Sottogruppi normali

Definizione 7.1. Un sottogruppo $N < G$ si dice *normale* se $gNg^{-1} \subset N$ per ogni $g \in G$.

Abbiamo visto a lezione la rilevanza dei sottogruppi normali: sono quelli per i quali l'operazione di gruppo in G definisce una buona operazione di composizione sull'insieme G/N delle classi laterali. Il teorema dimostrato a lezione era:

Teorema 7.2. *Sia N un sottogruppo di un gruppo G. Sono proprietà equivalenti di N:*

1. *$gNg^{-1} \subset N$ per ogni $g \in G$.*
2. *$gNg^{-1} = N$ per ogni $g \in G$.*
3. *Ogni classe laterale sinistra di N in G è anche una classe laterale destra.*
4. *La moltiplicazione $(aN) \cdot (bN) = abN$ è ben definita.*

Dimostrazione. (1) $\Rightarrow$ (2): Sappiamo già che $gNg^{-1} \subset N$; basta quindi mostrare che $N \subset gNg^{-1}$. Ma si può ottenere n come $g(g^{-1}ng)g^{-1}$. La normalità di N mostra che $n' = g^{-1}ng = g^{-1}n(g^{-1})^{-1}$ è un elemento di N, ed abbiamo quindi scritto $n = gn'g^{-1}$ per qualche $n' \in N$.
(2) $\Rightarrow$ (3): Mostriamo innanzitutto che $gN \subset Ng$. In effetti se $x \in gN$, allora $x = gn$ per qualche $n \in N$ e quindi $x = (gng^{-1})g \in Ng$. Viceversa, se $x \in Ng$, allora $x = ng$ per qualche $n \in N$ e quindi $x = gg^{-1}ng = g(g^{-1}n(g^{-1})^{-1}) \in gN$ e quindi $Ng \subset gN$.
(3) $\Rightarrow$ (4): Se X, Y sono sottoinsiemi di G, indichiamo con XY l'insieme dei prodotti $xy, x \in X, y \in Y$. Allora possiamo scrivere

$$(aN)(bN) = (aN)(Nb) = aNNb = aNb = a(Nb) = abN.$$

Questo mostra che scegliendo un elemento da aN e moltiplicandolo per un elemento di bN, si ottiene un risultato che appartiene sempre ad abN. In altre parole, la classe di congruenza modulo N di ab dipende solo dalle classi di congruenza di a e b. Pertanto il prodotto è ben definito.
(4) $\Rightarrow$ (1): Se la moltiplicazione è ben definita, allora $ab \equiv (an)(bn') \mod N$. Questo vuol dire che $(ab)^{-1}anbn' \in N$ per ogni $a, b \in G, n, n' \in N$. Ma $(ab)^{-1}anbn' = b^{-1}nbn'$. Ponendo $b = g^{-1}$ e $n' = 1$ si ottiene $gng^{-1} \in N$. □

Corollario 7.3. *Un sottogruppo di indice 2 è normale.*

Dimostrazione. Un sottogruppo $H < G$ di indice 2 ha solo due laterali destri. Uno di questi è H stesso, e l'altro non può che essere $G \setminus H$. Lo stesso ragionamento vale per i laterali sinistri. Perciò ogni laterale sinistro è anche destro, e $H \lhd G$. □

Esempi:

1. Ogni sottogruppo di un gruppo abeliano è normale.
2. A_n è un sottogruppo normale di S_n. Infatti, ha indice 2.
3. Se $\sigma = (12), H = (\sigma)$ allora H non è normale in S_3. Infatti $(13)(12)(13)^{-1} = (23) \notin H$.
4. Sia $H = \{e, (12)(34), (13)(24), (14)(23)\}$. Allora $H \lhd \mathrm{A}_4$. Vedremo in seguito che per $n \geq 5$ A_n non ha sottogruppi normali non banali.
5. Non è vero che se i sottogruppi di un gruppo sono tutti normali, il gruppo è necessariamente abeliano. Sia infatti Q_8 il gruppo delle unità dei quaternioni. I suoi sottogruppi di ordine 4 hanno indice 2, e sono normali. Vi è un solo sottogruppo di ordine 2, e precisamente $\{\pm 1\}$, che giace nel centro di Q_8 ed è quindi normale. Gli altri sottogruppi sono quelli banali, che sono automaticamente normali. Quindi ogni sottogruppo di Q_8 è normale, eppure Q_8 non è abeliano.

Abbiamo visto come il prodotto in G induca un'operazione sul quoziente G/N se $N \lhd G$.

Teorema 7.4. *L'operazione indotta da G su G/N definisce una struttura di gruppo.*

Dimostrazione. La dimostrazione è ovvia: $eN = N$ è l'identità, $g^{-1}N$ è l'inverso di gN. Inoltre il prodotto è associativo poiché $(aNbN)cN = abNcN = (ab)cN = a(bc)N = aN(bc)N = aN(bNcN)$. □

Si noti che se definiamo $\pi_N : G \to G/N$ come $\pi_N(g) = gN$, allora $\pi_N(ab) = \pi_N(a)\pi_N(b)$. Su questa proprietà è basato il concetto di omomorfismo.

Esercizi:
(a) Il centro Z di un gruppo G è un sottogruppo normale di G.
(b) Sia $H < G$. Il sottoinsieme $\{g \in G | gHg^{-1} = H\}$ è detto *normalizzatore* di H in G, e si indica con $N(H)$. Mostrate che $H \lhd N(H)$.
(c) Sia $H < G$. Mostrate che il sottoinsieme $\{g \in G | gHg^{-1} \subseteq H\}$ è un sottogruppo di G *se* G *è un gruppo finito*, ed in tal caso coincide con il normalizzatore di H in G.
(d) Sia G il sottoinsieme di $\mathrm{GL}_2(\mathbb{Q})$ costituito da tutte le matrici della forma

$$\begin{pmatrix} 2^k & q \\ 0 & 2^{-k} \end{pmatrix},$$

dove $k \in \mathbb{Z}, q \in \mathbb{Q}$, e sia

$$H = \left\{ \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix}, q \in \mathbb{Z} \right\} \subset G.$$

Mostrate che $H < G$, e che il sottoinsieme $\{g \in G | gHg^{-1} \subseteq H\}$ **non** è un sottogruppo di G.
(e) Sia $H < G$. Il centralizzatore di H in G è il sottoinsieme $C(H) = \{g \in G | gh = hg \text{ per ogni } h \in H\}$. Mostrate che $C(H)$ è un sottogruppo di G e che $C(H) \lhd G$ se $H \lhd G$.

8. Omomorfismi di gruppi

Siano $G, \overline{G}$ due gruppi, le cui identità indichiamo con $e, \bar{e}$ rispettivamente.

Definizione 8.1. $\phi : G \to \overline{G}$ è un *omomorfismo di gruppi*, o più semplicemente un *omomorfismo*, se

$$\phi(ab) = \phi(a)\phi(b)$$

per ogni scelta di $a, b \in G$. Un omomorfismo invertibile si dice *isomorfismo*, mentre un isomorfismo di un gruppo su se stesso si dice *automorfismo*.

Lemma 8.2. *Se $\phi : G \to \overline{G}$ è un omomorfismo di gruppi, allora $\phi(e) = \bar{e}, \phi(g^{-1}) = \phi(g)^{-1}$.*

Dimostrazione. Poiché $e \cdot e = e$ in G, si ha $\phi(e) = \phi(e \cdot e) = \phi(e) \cdot \phi(e)$. Moltiplicando a sinistra per l'inverso di $\phi(e)$ in $\overline{G}$ si ottiene $\phi(e) = \bar{e}$. Allo stesso modo, da $g \cdot g^{-1} = e$ segue $\bar{e} = \phi(e) = \phi(g \cdot g^{-1}) = \phi(g)\phi(g^{-1})$. Di conseguenza, $\phi(g^{-1})$ è l'inverso di $\phi(g)$. □

Esempi:
(1) L'applicazione che manda ogni elemento del gruppo G nell'identità di un altro gruppo è un omomorfismo.
(2) L'applicazione identità da un gruppo in sé è un omomorfismo. E' *l'automorfismo identico* del gruppo.
(3) L'applicazione $\mathrm{sgn} : \mathrm{S}_n \to \{\pm 1\}$ è un omomorfismo. Infatti $\mathrm{sgn}(\phi\psi) = \mathrm{sgn}(\phi)\,\mathrm{sgn}(\psi)$.
(4) L'applicazione $\det : \mathrm{GL}_n(\mathbf{k}) \to \mathbf{k}^*$ che manda ogni matrice M nel suo determinante $\det M \in \mathbf{k}^* = \mathbf{k} \setminus \{0\}$ è un omomorfismo. Infatti $\det(AB) = \det(A)\det(B)$.
(5) L'applicazione $\exp : \mathbb{R} \to \mathbb{R}^*$ definita come $\exp(x) = e^x$ è un omomorfismo di gruppi. Infatti l'operazione di gruppo di $\mathbb{R}$ è la somma, e si ha $\exp(x + y) = \exp(x)\exp(y)$.
(6) Se g è un elemento del gruppo G, $n \mapsto g^n$ definisce un omomorfimo $\mathbb{Z} \to G$. Infatti $g^m g^n = g^{m+n}$.
(7) Ogni spazio vettoriale può essere visto come gruppo abeliano rispetto alla sola operazione di somma tra vettori. Allora una applicazione lineare tra spazi vettoriali è sempre un omomorfismo di gruppi.

Definizione 8.3. Il *nucleo* di G è l'insieme degli elementi g di G tali che $\phi(g) = \bar{e}$. L'*immagine* di G è l'insieme degli elementi $\bar{g}$ di $\overline{G}$ per i quali esiste $g \in G$ tale che $\phi(g) = \bar{g}$.

Indicheremo il nucleo e l'immagine di un omomorfismo ϕ con $\ker\phi, \mathrm{Im}\phi$ rispettivamente. Una semplice verifica mostra che $\mathrm{Im}\phi$ è sempre un sottogruppo di $\overline{G}$, mentre $\ker\phi$ è un sottogruppo normale di G. Questi fatti ammettono un'immediata generalizzazione.

Proposizione 8.4. *Sia $\rho : G \to \overline{G}$ un omomorfismo di gruppi.*

- *Se $H < G$, allora $\rho(H) < \overline{G}$. Inoltre, se $H \lhd G$, allora $\rho(H) \lhd \rho(H)$.*
- *Se $\overline{H} < \overline{G}$, allora $\rho^{-1}(\overline{H}) < G$. Inoltre, se $\overline{H} \lhd \overline{G}$, allora $\rho^{-1}(\overline{H}) \lhd G$.*

Dimostrazione. Per quanto riguarda il primo enunciato, $x \in \rho(H)$ se e solo se esiste $h \in H$ tale che $x = \rho(h)$. Dal momento che ρ è un omomorfismo di gruppi, sappiamo che $\rho(h_1)\rho(h_2) = \rho(h_1h_2)$ e che $\rho(h)^{-1} = \rho(h^{-1})$. Questo mostra che $\rho(H) < \overline{G}$. Per mostrare che $\rho(H) \lhd \overline{G}$ se H è normale in G, basta invece osservare che $\rho(g)\rho(h)\rho(g)^{-1} = \rho(ghg^{-1}) \in \rho(H)$ per ogni $h \in H, g \in G$.

La dimostrazione del secondo enunciato si fa in maniera simile, osservando che $x \in \rho^{-1}(\overline{H})$ se e solo se $\rho(x) \in \overline{H}$. Allora da $x, y \in \rho^{-1}(\overline{H})$ segue $\rho(x), \rho(y) \in \overline{H}$, e quindi $\rho(xy) = \rho(x)\rho(y) \in \overline{H}$ da cui $xy \in \rho^{-1}(\overline{H})$. Allo stesso modo:

$$x \in \rho^{-1}(\overline{H}) \Rightarrow \rho(x) \in \overline{H} \Rightarrow \rho(x^{-1}) = \rho(x)^{-1} \in \overline{H} \Rightarrow x^{-1} \in \rho^{-1}(\overline{H}).$$

Per mostrare che se $\overline{H} \lhd \overline{G}$ allora $\rho^{-1}(\overline{H}) \lhd G$, basta osservare che la composizione $\pi \circ \rho$, dove $\pi : \overline{G} \to \overline{G}/\overline{H}$ è la proiezione al quoziente, è ancora un omomorfismo, ed il suo nucleo è precisamente $\rho^{-1}(\overline{H})$. (perché?) □

Esempi:

(1) L'applicazione identità da un gruppo in sé è un omomorfismo iniettivo; infatti solo l'identità giace nel suo nucleo. L'immagine coincide con l'intero gruppo.
(2) Il nucleo di $\mathrm{sgn} : \mathrm{S}_n \to \{\pm 1\}$ è il sottogruppo A_n delle permutazioni pari.
(3) Il nucleo di $\det : \mathrm{GL}_n(\mathbf{k}) \to \mathbf{k}^*$ è dato dal sottogruppo $\mathrm{SL}_n(\mathbf{k})$ delle matrici di determinante 1. L'immagine è tutto $\mathbf{k}^*$.
(4) L'omomorfismo $\exp : \mathbb{R} \to \mathbb{R}^*$ non è un isomorfismo. E' infatti iniettivo, poiché $e^x = 1 \Rightarrow x = 0$, ma non è suriettivo, poiché la sua immagine è il sottogruppo dei numeri reali positivi in $\mathbb{R}^*$.
(5) L'omomorfismo $\mathbb{Z} \ni n \mapsto g^n \in G$ ha per immagine il sottogruppo di G generato da g, e per nucleo il sottogruppo di $\mathbb{Z}$ generato da $o(g)$ se l'ordine di g è finito, e (0) se è infinito.
(6) La proiezione $\pi_N : G \to G/N$ è suriettiva, ed ha N come nucleo.

L'ultimo esempio in particolare ci dice che un sottogruppo è normale se e solo se è il nucleo di qualche omomorfismo.

Applicando la Proposizione 8.4 alla proiezione al quoziente $\pi : G \to G/N$, dove $N \lhd G$, si vede subito che $\pi(H) < G/N$ quando $H < G$, e che $\pi^{-1}(\overline{H})$ è un sottogruppo di G che contiene N, se $\overline{H} < G/N$.

Lemma 8.5. *Se $\pi : G \to G/N$ è la proiezione al quoziente per il sottogruppo normale N, allora $\pi(H) = \pi(HN)$.*

Dimostrazione. L'inclusione $\pi(H) \subset \pi(HN)$ è ovvia. Per mostra che $\pi(HN) \subset \pi(H)$ basta osservare che $[hn] = [h][n] = [h][e] = [h]$ per ogni $h \in H, n \in N$. □

Osservazione 8.6. Quando H contiene N, è naturale indicare con H/N la proiezione $\pi(H)$. Il lemma appena dimostrato ci dice che quando $N \not\subset H$, allora $\pi(H) = \pi(HN) = HN/N$.

Proposizione 8.7. *Sia $N \lhd G$, e $\pi : G \to G/N$ la proiezione al quoziente.*

- *Se $H < G$, allora $\pi^{-1}(\pi(H)) = HN$. In particolare, se $N \subset H$, allora $\pi^{-1}(\pi(H)) = H$.*
- *Se $\overline{H} < G/N$, allora $\pi(\pi^{-1}(\overline{H})) = \overline{H}$.*

Dimostrazione. Da $\pi(H) = \pi(HN)$ segue che $HN \subset \pi^{-1}(\pi(H))$. Per mostrare che $\pi^{-1}(\pi(H)) \subset HN$, basta osservare che $x \in \pi^{-1}(\pi(H))$ se e solo se $\pi(x) \in \pi(H)$, cioè se esiste $h \in H$ tale che $\pi(x) = \pi(h)$. Ma allora $h^{-1}x \in \ker \pi = N$, e quindi $x \in hN \subset HN$.

Per quanto riguarda la seconda affermazione, $\pi(\pi^{-1}(\overline{H})) = \overline{H} \cap \pi(G)$ che coincide con $\overline{H}$ per la suriettività di π. □

Teorema 8.8. *Sia $N \lhd G$, e $\pi : G \to G/N$ la proiezione al quoziente. Allora $H \mapsto \pi(H)$ costituisce una corrispondenza biunivoca tra i sottogruppi di G che contengono N e i sottogruppi di G/N. In tale corrispondenza, a sottogruppi normali di G corrispondono sottogruppi normali di G/N e viceversa.*

Dimostrazione. La Proposizione 8.7 mostra che $\overline{H} \mapsto \pi^{-1}(\overline{H})$ è un'inversa sia destra che sinistra di $H \mapsto \pi(H)$. L'affermazione sulla normalità segue dalla Proposizione 8.4. □

8.1. **Teorema di Cauchy nel caso abeliano.** Avendo introdotto i concetti di omomorfismo e gruppo quoziente, possiamo fornire una dimostrazione del Teorema di Cauchy per i gruppi abeliani finiti.

Lemma 8.9. *Se $x \in G$ ha ordine $n = dk$, allora $o(x^k) = d$. In particolare, se G possiede elementi di ordine n e d divide n, allora possiede anche elementi di ordine d.*

Dimostrazione. Sappiamo che n è il minimo esponente positivo tale che $x^n = e$. Poiché $(x^k)^d = x^{dk} = x^n = e$, concludiamo che x^k ha ordine d. □

Lemma 8.10. *Se $\phi : G \to \overline{G}$ è un omomorfismo di gruppi e $x \in G$ allora $o(\phi(x))$ divide $o(x)$. Se inoltre ϕ è iniettivo, allora $o(\phi(x)) = o(x)$.*

Dimostrazione. Se $o(x) = n$, allora $x^n = e$ e di conseguenza $\phi(x)^n = \phi(x^n) = \phi(e) = \overline{e}$. Per il Lemma precedente, $o(\phi(x))$ divide n. Se ϕ è iniettiva, $x^n = e$ se e solo se $\phi(x)^n = \overline{e}$ e quindi x e $\phi(x)$ hanno lo stesso ordine. □

Teorema 8.11. *Sia G un gruppo abeliano finito e p un primo che divide $|G|$. Allora G contiene almeno un elemento di ordine p.*

Dimostrazione. Per induzione su $|G| > 1$, la base dell'induzione $|G| = 2$ essendo ovvia.

Scegliamo $e \neq g \in G$. Il sottogruppo (g) è normale e possiamo considerare il quoziente $G/(g)$. Ora $|G| = |(g)| \cdot |G/(g)|$ pertanto p divide $o(g)$ oppure $|G/(g)|$. Se p divide $o(g)$ abbiamo finito per il Lemma 8.9. Se invece p divide $|G/(g)| < |G|$, possiamo usare l'ipotesi induttiva su $G/(g)$ e concludere che $G/(g)$ possiede almeno un elemento di ordine p.

Se $\pi : G \to G/(g)$ indica la proiezione al quoziente, e $x \in G$ è tale che $\pi(x)$ ha ordine p, allora $o(x)$ è multiplo di p per il Lemma 8.10, e concludiamo nuovamente utilizzando il Lemma 8.9. □

9. TEOREMI DI OMOMORFISMO

Il teorema che segue è l'analogo gruppale di un enunciato riguardante le relazioni di equivalenza su insieme dimostrato all'inizio del corso.

Teorema 9.1. *Sia N un sottogruppo normale di un gruppo G, ed $f : G \to H$ un omomorfismo di gruppi tale che $N \subset \ker f$. Allora esiste un unico omomorfismo di gruppi $F : G/N \to H$ tale che, indicata con $\pi : G \to G/N$ la proiezione al quoziente, si abbia $f = F \circ \pi$.*

Inoltre F è suriettiva se e solo se f è suriettiva, ed F è iniettiva se e solo se $N = \ker f$.

Dimostrazione. Mostriamo innanzitutto l'unicità di F. Dal momento che $\pi(g) = [g] = gN$, se F soddisfa l'enunciato del teorema, deve valere $F([g]) = f(g)$ per ogni $g \in G$. Rimane da controllare che tale applicazione F sia ben definita, e che sia effettivamente un omomorfismo.

Per controllare la buona definizione di F, è sufficiente verificare che se $[g_1] = [g_2]$, allora $f(g_1) = f(g_2)$. Sappiamo che $[g_1] = [g_2]$ se e solo se $g_1 \equiv g_2 \mod N$, cioè esattamente quando $g_1^{-1}g_2 \in N$. Ma allora $f(g_2) = f(g_1 g_1^{-1} g_2) = f(g_1)f(g_1^{-1}g_2) = f(g_1) \cdot \bar{e} = f(g_1)$, poiché $N \subset \ker f$. Se è ben definita, F è chiaramente un omomorfismo. In effetti

$$F([a][b]) = F([ab]) = f(ab) = f(a)f(b) = F([a])F([b]),$$

per ogni $a, b \in G$.

Per quanto riguarda l'affermazione sulla suriettività, è sufficiente ricordare che la proiezione $\pi : G \to G/N$ è sempre suriettiva. Quando F è suriettiva, $f = F \circ \pi$ è composizione di applicazioni suriettive, ed è pertanto suriettiva. Viceversa, se la composizione $f = F \circ \pi$ è suriettiva, la prima applicazione nella composizione deve essere suriettiva.

Per quanto invece concerne l'iniettività di F, si vede facilmente che $\ker F = \{[a] \in G/N | f(a) = e\} = \pi(\ker f)$. Poiché $N \subset \ker f$, si ha $\pi(ker f) = \{[e]\}$ se e solo se $\ker f = N$. □

Osservazione 9.2. Il teorema appena dimostrato richiede qualche spiegazione sulle sue possibili applicazioni. E' intanto ovvio che se conosciamo un omomorfismo di gruppi $F : G/N \to H$, possiamo costruire la composizione $f = F \circ \pi$, e questa è nuovamente un omomorfismo $f : G \to H$, che per costruzione contiene N nel suo nucleo.

Il teorema ci spiega che questa costruzione può essere invertita: ogni omomorfismo $f : G \to H$ che contenga N nel suo nucleo si ottiene nel modo appena descritto, ed inoltre si ottiene in tal modo per *precisamente una scelta* di $F : G/N \to H$. In altre parole, esiste una corrispondenza biunivoca tra gli omomorfismi da G in H che contengono N nel loro nucleo, e gli omomorfismi da G/N in H. Che cosa vuol dire esattamente quest'affermazione?

Evidentemente, se abbiamo bisogno di costruire un omomorfismo $G/N \to H$ e questo è difficile da fare direttamente, possiamo limitarci a costruire un omomorfismo $G \to H$ — la qual cosa potrebbe rivelarsi più semplice — e poi semplicemente verificare che N è contenuto nel suo nucleo.

Esempio. Costruiamo tutti gli omomorfismi dal gruppo $(\mathbb{Z}/(15), +)$ al gruppo $(\mathbb{Z}/(10), +)$. Il gruppo $\mathbb{Z}/(15)$ è quoziente di $\mathbb{Z}$ per il sottogruppo normale generato da 15 — può valere la pena di ricordare che ogni sottogruppo di $\mathbb{Z}$ è normale, dal momento che $\mathbb{Z}$ è un gruppo abeliano.

Per il Teorema 9.1, alla luce dell'Osservazione 9.2, è sufficiente costruire tutti gli omomorfismi $f : \mathbb{Z} \to \mathbb{Z}/(10)$ che contengano il sottogruppo (15) nel loro nucleo.

Tutti gli omomorfismi da $\mathbb{Z}$ in un gruppo G si costruiscono scegliendo un elemento $g \in G$ e ponendolo come immagine di $1 \in \mathbb{Z}$: sono in altre parole della forma $\phi(n) = g^n$ per ogni $n \in \mathbb{Z}$. Un elenco completo di omomorfismi $f : \mathbb{Z} \to \mathbb{Z}/(10)$ è quindi dato da $f(n) = [an]$, con $[a] \in \mathbb{Z}/(10)$.

Ora dobbiamo comprendere quali di tali omomorfismi (uno per ogni $[a]$) *scendano al quoziente*, cioè fattorizzino attraverso la proiezione al quoziente. Conosciamo già la condizione da verificare, e cioè che (15) sia contenuto nel nucleo di f. Dal momento che (15) è generato da 15, è sufficiente controllare quando 15 appartenga al nucleo, cioè quando $f(15) = [0]$.

Ma questo accade esattamente quando $15a \equiv 0 \mod 10$, cioè quando $3a \equiv 0 \mod 2$ cioè quando $a \equiv 0 \mod 2$. Vanno scelte quindi le classi $[a] \in \mathbb{Z}/(10)$ con a pari, il che fornisce gli omomorfismi:

- $f(n) = [0]$,
- $f(n) = [2n]$,
- $f(n) = [4n]$,
- $f(n) = [6n]$,
- $f(n) = [8n]$.

9.1. **Conseguenze del Teorema 9.1.**

Teorema 9.3. *Se $f : G \to H$ è un omomorfismo di gruppi, allora la sua immagine $f(G)$ è isomorfa al quoziente $G/\ker f$.*

Dimostrazione. A meno di sostituire H con $f(G)$, possiamo supporre che f sia suriettiva. Applicando il Teorema 9.1 ad $N = \ker f$ si ottiene una $F : G/N \to f(G)$ che è sia iniettiva che suriettiva, cioè un isomorfismo. □

Teorema 9.4. *Se $H, N \lhd G$, con $N \subset H$, allora $H/N \lhd G/N$ ed i quozienti G/H e $(G/N)/(H/N)$ sono isomorfi.*

Dimostrazione. Applichiamo il Teorema 9.1 all'omomorfismo $f = \pi_H : G \to G/H$ di proiezione al quoziente, e al sottogruppo $N \subset \ker f = H$. Risulta individuato un unico omomorfismo $F : G/N \to G/H$ tale che[7] $F(gN) = gH$ per ogni $g \in G$, che è suriettivo per la suriettività di f.

[7]Sono purtroppo costretto ad indicare $[g]$ con gN oppure gH, per evitare ambiguità di notazione.

Il nucleo di F è $\ker F = \{gN \in G/N | gH = H\} = \{gN \in G/N | g \in H\} = H/N$. Questo mostra che H/N è un sottogruppo normale di G/N (come seguiva anche dalla Proposizione 8.4) in quanto nucleo di un omomorfismo, e per il Teorema 9.3 si ha: $G/H = \mathrm{Im}F = (G/N)/\ker F = (G/N)/(H/N)$. □

Teorema 9.5. *Se H, N sono sottogruppi di G, con $N \lhd G$, allora vi è un isomorfismo tra HN/N e $H/H \cap N$*

Dimostrazione. Sia $\pi : G \to G/N$ l'omomorfismo di proiezione al quoziente. La restrizione — chiamiamola f — di π ad H è ancora un omomorfismo $f : H \to G/N$ la cui immagine coincide, grazie all'Osservazione 8.6, con HN/N.

E' facile calcolare il nucleo di f; infatti $\ker f = \{h \in H | [h] = [e]\} = H \cap N$, il che mostra che $H \cap N$ è normale in H. Per il Teorema 9.3 si ha allora che $HN/N = \mathrm{Im}f = H/\ker f = H/H \cap N$. □

I tre teoremi appena illustrati sono solitamente detti primo, secondo e terzo teorema di omomorfismo per i gruppi. Vediamone due facili applicazioni.

Proposizione 9.6. *L'ordine di $[a]$ nel gruppo (additivo) $\mathbb{Z}/(n)$ è uguale a $n/\mathrm{MCD}(a, n)$.*

Dimostrazione. Un'osservazione preliminare: dal momento che l'operazione di gruppo in $\mathbb{Z}$ è indicata additivamente, il prodotto di sottogruppi sarà indicato con $H + K$ e non con HK.

Indichiamo con $\pi : \mathbb{Z} \to \mathbb{Z}/(n)$ la proiezione al quoziente. Se $K = (a)$ e $N = (n)$, allora $\pi(K) = \pi(K + N) = (K + N)/N$; d'altronde il sottogruppo generato in $\mathbb{Z}/(n)$ da $[a]$ è esattamente $\pi(K)$. Sappiamo già che $K + N$ è il sottogruppo generato dal massimo comun divisore $\mathrm{MCD}(a, n)$.

Ricapitolando, se $G = \mathbb{Z}$, $H = K + N = (\mathrm{MCD}(a, n))$, $N = (n)$, allora $G/N = \mathbb{Z}/(n)$ e $H/N = ([a])$. Dal secondo teorema di omomorfismo si ottiene $G/H \simeq (G/N)/(H/N)$, cioè $\mathbb{Z}/(a, n) \simeq (\mathbb{Z}/(n))/([a])$. Ora, il gruppo $\mathbb{Z}/(\mathrm{MCD}(a, n))$ possiede $\mathrm{MCD}(a, n)$ elementi, mentre il gruppo $\mathbb{Z}/(n)$ ne possiede n. Per il teorema di Lagrange, il sottogruppo $([a])$ deve contenere allora $n/\mathrm{MCD}(a, n)$ elementi, e quindi l'ordine di $[a]$ in $\mathbb{Z}/(n)$ è $n/\mathrm{MCD}(a, n)$. □

Proposizione 9.7. *Siano $a, b \in \mathbb{Z}$ elementi non nulli. Allora il minimo comune multiplo di a e b è dato da $ab/\mathrm{MCD}(a, b)$.*

Dimostrazione. Siano $H = (a), N = (b)$ sottogruppi di $\mathbb{Z}$. Se d è il loro massimo comun divisore, ed m è il loro minimo comune multiplo, allora sappiamo già che $H + N = (d), H \cap N = (m)$.

Per il terzo teorema di omomorfismo, abbiamo allora $H+N/N \simeq H/H \cap N$, cioè $(d)/(b) = (a)/(m)$. Confrontando le cardinalità dei due quozienti[8] si ottiene $m = ab/d$. □

E-mail address: dandrea@mat.uniroma1.it

[8]Attenzione: la cardinalità di $(d)/(b)$ è b/d e quella di $(a)/(m)$ è m/a!!!