Von Neumann: dalle rappresentazioni lineari di gruppi compatti al quinto problema di Hilbert

Luca Tamanini

28 maggio 2012

Indice

[1] Sulle proprietà analitiche di gruppi di trasformazioni lineari e delle loro rappresentazioni, cfr. [14].

Capitolo 1

Introduzione

Wir müssen wissen. Wir werden wissen.
David Hilbert

1.1 L'alba del nuovo secolo

L'Ottocento cedeva il passo al Novecento e il nuovo secolo si apriva all'insegna del fervore culturale, del rinnovamento di ogni ambito dello scibile umano. Il "secolo breve" si destava con la morte conclamata del Positivismo filosofico di Comte, già annunciata da Nietzsche, e la rivalutazione dello scetticismo, con la pubblicazione de *L'interpretazione dei sogni* di Sigmund Freud, che avrebbe dato il via alla psicanalisi, e di lì a breve, nel 1904, avrebbe visto la luce l'articolo *Zur Elektrodynamik der bewegten Körper*, pietra miliare di Albert Einstein nella fondazione della teoria della relatività speciale. In questo preciso contesto storico, la matematica si trovava impegnata nella più radicale ristrutturazione del suo assetto logico e formale: volgeva infatti al termine un'era caratterizzata da un uso disinibito e privilegiato dell'intuizione pura, mentre andava sempre più maturando la necessità di una via assiomatica alla materia.

Simboli di queste due anime, contrapposte e pur complementari, della matematica furono Henri Poincarè (1854-1912) e David Hilbert (1862-1943) e non a caso i due più eminenti matematici dell'epoca furono chiamati a proporre una lettura al Primo e al Secondo Congresso Internazionale dei Matematici rispettivamente, svoltisi a Zurigo nel 1897 e a Parigi nel 1900. E mentre il matematico transalpino era strenuo sostenitore della forza dell'intuizione sull'assiomatica purista, la mattina dell'8 agosto del 1900, dopo essersi consultato con gli amici Hermann Minkowski (1864-1909) e Adolf Hurwitz (1859-1919), David Hilbert, colui che era considerato la guida dei matematici della sua generazione per l'innegabile carisma, tenne la sua lettura alla Sorbona a riguardo dei futuri problemi della matematica. Per questioni di tempistica, Hilbert espose solo dieci dei problemi proposti, ma un primo riassunto del testo, tradotto in francese, apparve nello stesso anno sul giornale svizzero *L'Enseignement Mathèmatique*[1] e contemporaneamente l'originale tedesco fu pubblicato negli annali dell'Università di Göttingen[2]. L'anno successivo il testo fu dato ancora alle stampe, con l'aggiunta di tre nuovi problemi, nell'*Archiv der Mathematik und Physik*[3], mentre il preambolo e dieci dei problemi presenti in quest'ultima versione apparvero in un testo francese anonimo su *Revue Gènèrale des Sciences Pures et Appliquèes*[4]. Nel 1902, il matematico francese Lèonce Laugel tradusse la versione completa dell'*Archiv*, che comparve nei rendiconto del Congresso[5] e come pamphlet non datato con il titolo generico *Mathematical Problems*. Infine, un'ultima traduzione inglese fu preparata per il *Bulletin of the American Mathematical Society*[6] da Mary Newson (1869-1959).

Dopo aver così trattato la genesi e l'evoluzione di quello che è a tutti gli effetti un manifesto programmatico di matematica, si può ora affrontare il suo contenuto.

1.2 I 23 problemi di Hilbert

> *Who of us would not be glad to lift the veil behind which the future lies hidden; to cast a glance at the next advances of our science and at the secrets of its development during future centuries? What particular goals will there be toward which the leading mathematical spirits of coming generations will strive? What new methods and new facts in the wide and rich field of mathematical thought will the new centuries disclose?*

Hilbert apre con queste parole la sua lettura: parole che stigmatizzano la curiosità propria dello spirito matematico e la ricerca di un confronto continuo con nuovi problemi. Il matematico tedesco, infatti, passa ben presto a sottolineare l'importanza precipua svolta da singoli problemi per lo sviluppo della matematica, il fatto che sia la loro presenza a mantenere in vita le svariate branche della scienza, e a tal riguardo riporta tre esempi significativi: il problema della brachistocrona di Bernoulli, la cui risoluzione gettò le basi per il calcolo delle variazioni, il problema di Fermat[7], che a lungo ha tormentato i matematici di tutto il mondo e che spinse Kummer a introdurre i numeri ideali, promuovendo così la teoria dei numeri, e infine il problema a tre corpi, di vitale importanza in fisica matematica e nei problemi di meccanica celeste. Spesso la nascita di tali problemi, come sostenuto da Hilbert, è motivata da esigenze fisiche, ma accanto

[1] David Hilbert, *Problèmes mathèmatiques*, l'Ens. Math. 2, pp. 349-355 (1900)

[2] David Hilbert, *Mathematische Probleme*, Nachrichten Königlichen Gesellschaft Wissenschaften Göttingen, math.-physik. Klasse, pp. 253-297 (1900)

[3] David Hilbert, *Mathematische Probleme*, Arch. Math. Physik 1, 4463, pp. 213-237 (1901)

[4] David Hilbert, *Problmes mathmatiques*, Revue Gèn. Sci. Pures Appl. 12, pp. 168-174 (1901)

[5] David Hilbert, *Sur les problèmes futurs des mathèmatiques*, pp. 58-114 (1902)

[6] David Hilbert, *Mathematical problems*, Bull. Amer. Math. Soc. 8, pp. 437-479 (1902)

[7] Per $n \geq 3$, l'equazione diofantea $x^n + y^n = z^n$ non ammette soluzioni.

a questa fase "primordiale" di genesi ve n'è anche una seconda, che si manifesta quando il libero pensiero si rende indipendente dalla fisica[8]. Si giustifica in questo modo la presenza di nature completamente differenti nei seguenti 23 problemi, che negli intenti di Hilbert dovevano offrire, con la loro risoluzione, particolari sviluppi alla matematica.

1. Il problema di Cantor dei numeri cardinali del continuo: si affrontano alcuni aspetti basilari di teoria degli insiemi, come l'ipotesi del continuo e il principio del buon ordinamento.

2. La compatibilità degli assiomi dell'aritmetica: la questione principale si focalizza sulla necessità di indagare le relazioni sussistenti tra i vari assiomi dell'aritmetica, determinando se vi siano eventuali parti in comune e, soprattutto, se questi siano nascostamente contraddittori.[9]

3. L'uguaglianza dei volumi di due tetraedri di uguali basi e uguali altezze: è un problema di natura squisitamente geometrica che interessa l'utilizzo del metodo di esaustione in teoremi di geometria solida.

4. Il problema della linea retta come distanza più breve tra due punti: non poteva non esserci riferimento in questa lista ai recenti sviluppi delle geometrie non euclidee, condotti da Riemann, Lobachevsky e Minkowski.

5. La definizione di gruppo continuo di trasformazioni secondo Lie[10] senza l'assunzione di differenziabilità delle funzioni che definiscono il gruppo: senza questa, quanto ci si può avvicinare al concetto di gruppo di Lie?[11] E fino a che punto si possono invece indebolire le ipotesi sul gruppo, affinché restino validi tutti i risultati provati nel caso di funzioni di transizione analitiche?[12] Il problema può altresì porsi nei seguenti termini: un gruppo continuo di trasformazioni è automaticamente differenziabile e, dunque, un gruppo di Lie?

[8] *But, in the further development of a branch of mathematics, the human mind, encouraged by the success of its solutions, becomes conscious of its independence. It evolves from itself alone, often without appreciable influence from without, by means of logical combination, generalization, specialization, by separating and collecting ideas in fortunate ways, new and fruitful problems, and appears then itself as the real questioner.*

[9] Durante la relazione di Hilbert al Congresso di Parigi vi furono poche osservazioni sollevate, ma una di queste è dovuta a Giuseppe Peano a riguardo del secondo problema. Egli, infatti, riteneva che un sistema con le proprietà cercate fosse già stato formulato dai suoi compatrioti Burali-Forti, Padoa e Pieri e che in particolare la relazione *Un nuovo sistema di postulati irriducibili per l'algebra* di Padoa avrebbe risposto positivamente al problema. D'altra parte è comprovato che la scarsa conoscenza dell'italiano da parte di Hilbert abbia portato quest'ultimo a trascurare, se non addirittura ignorare, i contributi più significativi dei geometri italiani.

[10] Nel linguaggio moderno essi sono meglio noti come *gruppi di Lie.*

[11] *How far Lie's concept of continuous groups of transformations is approachable in our investigations without the assumption of the differentiability of the functions?*

[12] *In how far are the assertions which we can make in the case of differentiable functions true under proper modifications without this assumption?*

6. La trattazione matematica degli assiomi della fisica: si stimola un approccio assiomatico anche per le scienze fisiche in cui la matematica gioca un ruolo importante, *in primis* la teoria delle probabilità e la meccanica.

7. L'irrazionalità e la trascendenza di certi numeri: si propongono alcune asserzioni, una in particolare legata alle costruzioni con riga e compasso, non ancora provate legate all'argomento proposto.

8. I problemi dei numeri primi: si affronta la celebre ipotesi di Riemann, affermando che la sua prova potrà poi giovare ad uno studio più approfondito del logaritmo integrale come della congettura di Goldbach. Infine si suggerisce di applicare i risultati ottenuti in questa sede alla distribuzione di ideali primi in un campo.

9. La dimostrazione della Legge di Reciprocità, nel caso più generale, in ogni campo di numeri.

10. La determinazione della risolubilità di un'equazione diofantea.

11. Forme quadratiche con coefficienti numerici algebrici.

12. L'estensione del teorema di Kronecker sui campi abeliani ad ogni dominio di razionalità algebrico: si richiede una generalizzazione della teoria delle estensioni di campi a domini razionali arbitrari.

13. L'impossibilità di risolvere l'equazione generica di settimo grado con funzioni di solo due argomenti: mentre Abel e Galois a inizio Ottocento avevano mostrato l'impossibilità di risolvere per radicali la generica quintica e quindi anche le equazioni di grado superiore, successivamente d'Ocagne affrontò il problema di risolvere equazioni con medie di curve dipendenti da parametri arbitrari[13]. Ebbene, è possibile risolvere la generica equazione di settimo grado con l'ausilio di funzioni continue dipendenti da solo due parametri?

14. La prova della finitezza di certi sistemi completi di funzioni, ovvero invarianti e covarianti di sistemi di funzioni razionali.

15. La fondazione rigorosa del calcolo enumerativo di Schubert.

16. La topologia delle curve algebriche e delle superfici.

17. L'espressione di forme definite tramite quadrati, ovvero la riduzione di forme quadratiche a somme di quadrati.

18. Il riempimento dello spazio con poliedri congruenti: dopo aver posto la domanda se anche nello spazio euclideo n-dimensionale esista un numero finito di gruppi di moti con regioni fondamentali associate, ci si interroga sulla possibilità di riempire lo spazio per giustapposizione di poliedri, ovvero si indaga l'esistenza di un poliedro non regolare e *space-filling*. Indi

[13] d'Ocagne, *Traitè de Nomographie*, Parigi, 1899

si passa allo studio delle funzioni caratterizzate da equazioni differenziali ordinarie o a derivate parziali.

19. Analiticità delle soluzioni per problemi regolari nel calcolo delle variazioni: tale analiticità è necessaria?

20. Il problema generale con valori al contorno, meglio noto come problema di Dirichlet.

21. La dimostrazione dell'esistenza di equazioni differenziali lineari aventi un assegnato gruppo di monodromia.

22. L'uniformazione di relazioni analitiche tramite funzioni automorfe.

23. Ulteriori sviluppi dei metodi del calcolo delle variazioni: si sollevano alcune questioni importanti tra i particolari problemi aperti di questa branca della matematica, che a inizio Novecento si trovava in piena fioritura.

In particolare, si deve osservare come a problemi che sono veramente tali, nel senso più immediato e comune del termine, eminentemente "pratici", si affianchino anche problemi di natura programmatica e fondazionale: questo non deve stupire, perché Hilbert era convinto che la risoluzione di problemi procedesse di pari passo con l'assiomatizzazione della teoria. Ed è proprio quest'ultimo aspetto che viene ribadito con insistenza, ripetuto più e più volte come un mantra: la ricerca di basi solide su cui costruire l'edificio della matematica è l'unica via per progredire nella conoscenza. Per tale motivo Hilbert si sofferma anche sull'importanza di definire con chiarezza cosa sia un problema, in che modo questo debba essere espresso e come debba essere risolto; più nello specifico si richiede che sia possibile verificare la correttezza della soluzione in un numero finito di passi e sotto un numero finito di ipotesi[14]. In più il matematico tedesco fuga ogni dubbio sul fatto che solo l'analisi e l'aritmetica possano essere trattate formalmente: egli auspica anzi che il formalismo possa estendersi a tutte le discipline del sapere matematico ma anche fisico. Così, in quest'ottica di ricerca continua verso l'alto ma mai lasciata in balìa dell'istinto, di indagine radicale dei pilastri del sapere illuminata dall'esattezza e dalla sicurezza date solo dagli assiomi, il pensiero di Hilbert giunge al culmine nel seguente passo:

> *This conviction of the solvability of every mathematical problem is a powerful incentive to the worker. We hear within us the perpetual call : There is the problem. Seek its solution. You can find it by pure reason, for in mathematics there is no ignorabimus.*

E poco importa se l'ironia volle che nel 1931, poco prima che fossero pronunciate le storiche parole *Wir müssen wissen. Wir werden wissen*, il logico austriaco Kurt Gödel aveva dimostrato il teorema di incompletezza che avrebbe poi portato il suo nome. Il naufragio della visione, forse eccessivamente positivistica,

[14] *I should say first of all, this: that it shall be possible to establish the correctness of the solution by means of a finite number of steps based upon a finite number of hypotheses which are implied in the statement of the problem and which must always be exactly formulated.*

di Hilbert della matematica era solo parziale: la necessità di un assetto logico-formale rigoroso era innegabile e, fatto decisamente significativo, restava e resta tuttora valido il forte stimolo alla ricerca di nuovi problemi con cui misurarsi, il più potente incentivo al progresso del sapere.

A questo punto si affrontino più nel dettaglio tre dei precedenti problemi, tra cui rientra ovviamente il quinto, sul quale verte questa trattazione.

1.2.1 Il primo problema

Lo studio delle proprietà insiemistiche di uso comune in matematica è relativamente recente e dovuto in larga parte, ai suoi albori, a Georg Cantor. Solo nell'Ottocento, infatti, si sentì la necessità di indagare più a fondo sulla natura delle entità apparentemente più banali della matematica: i numeri. Già Galileo Galilei aveva fatto notare come i quadrati perfetti potessero essere messi in biezione con i naturali, per quanto potessero ingenuamente sembrare di meno. Ma con Cantor le speculazioni sugli insiemi transfiniti portarono a conclusioni alle quali lo stesso matematico stentava a credere. Infatti non solo $\mathbb{N}$ e $\mathbb{Z}$ avevano la stessa cardinalità, o equivalentemente lo stesso numero cardinale (in generale, infatti, due insiemi A e B hanno la stessa cardinalità se tra i due esiste una biezione), ma lo stesso poteva dirsi anche rispetto all'insieme dei numeri razionali $\mathbb{Q}$. Al contrario lo stesso Cantor mostrò che i reali $\mathbb{R}$ non potevano in alcun modo essere messi in corrispondenza biunivoca con $\mathbb{N}$ e che, anzi, la cardinalità di $\mathbb{R}$ era pari a $2^{\aleph_0}$, ove $\aleph_0 = |\mathbb{N}|$. Per questo motivo il matematico tedesco ipotizzò che non vi fosse alcun insieme, la cui cardinalità fosse strettamente compresa tra quella dei naturali e quella dei reali, ovvero

$$\nexists A \, : \, \aleph_0 < |A| < 2^{\aleph_0}$$

Il nome dell'ipotesi, abbreviato anche in CH, deriva dal fatto che la retta su cui sono usualmente rappresentati i reali è detta *continuo*, per l'appunto. Quando Hilbert stese la lista contenente i ben noti 23 problemi, l'ipotesi del continuo era ancora un problema aperto, una mera supposizione; ma con Gödel in primis e in ultima istanza con P. J. Cohen si giunse a fornire una risposta esauriente alla domanda, per quanto non nello spirito di quanto profetizzato da Hilbert. Nel 1940, infatti, il logico austriaco mostrò che CH non poteva essere dimostrata falsa usando la teoria assiomatica di Zermelo-Fraenkel con l'aggiunta dell'assioma di scelta. Nel 1963, invece, Cohen provò che CH non poteva nemmeno essere dimostrata vera all'interno della stessa teoria: tale ipotesi era, dunque, formalmente indecidibile. Questo fatto non è di per sè contraddittorio, ma anzi del tutto plausibile per quanto afferma il teorema di incompletezza di Gödel; esso resta però un risultato disturbante, in quanto è stato storicamente la prima affermazione alla quale si è dimostrato essere incapaci di rispondere affermativamente o negativamente. Lo stesso risultato di indecidibilità si applica inoltre all'ipotesi generalizzata del continuo (GCH), la quale afferma che se un insieme B ha cardinalità compresa tra quella di un insieme infinito A e quella del suo insieme delle parti $\mathcal{P}(A)$, allora $|B| = |A|$ oppure $|B| = |\mathcal{P}(A)|$. Equivalentemente, se A è un insieme di cardinalità infinita, si può dire che

$$\nexists B\,:\,|A| < |B| < 2^{|A|}$$

Successivamente al risultato di Cohen, visto che dall'ipotesi del continuo dipendono alcuni riusltati di analisi matematica, topologia e teoria della misura, si è mostrato anche l'indipendenza di questi dalla teoria degli insiemi ZFC.

1.2.2 Il quinto problema

Storicamente, il concetto di *gruppo di Lie* nacque ad opera di Sophus Lie nel contesto specifico di quelli che erano allora noti come *gruppi continui di trasformazioni*; solo successivamente si è sviluppata una loro teoria astratta. Nel linguaggio moderno, un gruppo di Lie non è altro che un gruppo topologico con la struttura di varietà analitica e infatti lo stesso Lie, fornendo una prima assiomatizzazione del concetto, richiedeva esplicitamente l'analiticità delle funzioni definenti il gruppo.[15] Ma già nel 1893, il matematico Friedrich H. Schur (1856 - 1932) aveva mostrato come fosse sufficiente richiedere che il gruppo topologico in questione fosse solamente una varietà di classe C^2, affinché fosse una varietà analitica. Quando la scoperta di Schur giunse sotto gli occhi di Hilbert, quest'ultimo si domandò se fosse possibile indebolire ulteriormente la richiesta di regolarità C^2 e per questo decise di inserire tale domanda tra i ventitrè problemi che avrebbe in seguito presentato a Parigi.

> *How far Lie's concept of continuous groups of transformations is approachable in our investigations without the assumption of the differentiability of the functions.*

All'epoca tale problema si poteva altresì formulare come di seguito: dato un certo gruppo continuo G di trasformazioni, allora esistono opportuni intorni U, V dell'identità e per cui risulta definita una mappa continua $F : V \times V \to U$; come mostrare, se possibile, che F è liscia? Infatti, come si vedrà nel seguito, i gruppi topologici sono omogenei e quindi il loro comportamento in un intorno dell'unità determina la loro natura ovunque. Con termini forse più comprensibili e odierni, la domanda si pone nel seguente modo.

> *Se un gruppo topologico è localmente euclideo (e dunque una varietà topologica), allora è anche un gruppo di Lie e dunque una varietà analitica?*

Le prime risposte, per quanto particolari e non generali, giunsero a cavallo degli Anni Venti e Trenta, ad opera di John von Neumann (1903-1957); nel 1929, infatti, egli dimostrò che ogni sottogruppo chiuso di un gruppo lineare generale è un gruppo di Lie e tale teorema è rimasto forse tra i più noti del grande

[15] Tali funzioni sono quindi gli elementi del gruppo e per queste era richiesta l'analiticità da parte di Lie. Nell'interpretazione corrente del quinto problema di Hilbert invece, in cui gli elementi del gruppo sono astratti, l'analiticità che deve essere provata è quella delle funzioni continue definite sul gruppo, ma questa visione non è in contrasto con la precedente, bensì la generalizza.

matematico ungherese. In seguito, nel 1933, provò il quinto problema di Hilbert nel caso in cui il gruppo topologico in questione, oltre ad essere localmente euclideo, fosse anche compatto, sfruttando le misure di Haar, che da poco avevano fatto la loro comparsa sul panorama matematico. Poco dopo, nel 1934, il russo Lev Pontryagin (1908-1988) dimostrò anche il caso di un gruppo abeliano localmente compatto. Ma per una risposta più generale al quesito posto da Hilbert si dovette attendere il secondo dopoguerra e più precisamente gli Anni Cinquanta. Grazie ai lavori di Andrew Gleason (1921-2008), Hidehiko Yamabe (1923-1960), Deane Montgomery (1909-1992) e Leo Zippin (1905-1995) si riuscì a rispondere definitivamente al quinto problema, in quella che generalmente è la sua interpretazione più diffusa. Infatti nel 1952 Gleason mostrò la risolubilità in positivo del problema nel caso di gruppi topologici che non contengono sottogruppi piccoli, la famosa *no small subgroups property*; nel 1953 Yamabe giunse allo stesso risultato e in più mostrò che un gruppo connesso localmente compatto è il limite proiettivo di un sistema proiettivo di gruppi di Lie. Sempre nel 1952 Montgomery e Zippin, nel loro articolo apparso negli *Annals of Mathematics*, dimostrarono che nessun gruppo topologico localmente euclideo contiene sottogruppi piccoli.

In questo modo il problema era risolto.

Vi è però una seconda interpretazione del quinto problema di Hilbert, che conduce direttamente alla congettura ancora aperta di Hilbert-Smith.

> *Un gruppo topologico che agisce in modo continuo su una varietà è necessariamente un gruppo di Lie?*

Appare evidente che in quest'ottica il problema di Hilbert è stato interpretato in un modo che risulta essere più vicino al significato primigenio di gruppo di Lie, inteso dunque come gruppo di trasformazioni. E in quanto tale, si è naturalmente propensi a far agire un gruppo di Lie su enti matematici quali le varietà.

1.2.3 L'ottavo problema

I testi divulgativi sull'ipotesi di Riemann si sprecano e forse uno dei più noti è *L'enigma dei numeri primi* di Marcus du Sautoy[16]; grazie a questi, anche tra i non addetti ai lavori si è sviluppata la consapevolezza di essere di fronte a uno dei problemi sicuramente più longevi della matematica, in quanto rimasto perfettamente inviolato dalla sua formulazione nel 1859, presentato da Hilbert al Congresso Internazionale dei Matematici del 1900 e riproposto come uno dei *Millennium Problems* dal Clay Mathematics Institute. Nell'anno menzionato, a Göttingen, Bernhard Riemann affermò che gli zeri cosiddetti *non banali* (e dunque diversi dagli zeri banali dati dagli interi negativi pari) della funzione zeta

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$$

[16] Marcus du Sautoy, *L'enigma dei numeri primi*, Rizzoli, Milano, 2004

dovessero avere tutti parte reale pari a $\frac{1}{2}$, ovvero si dovessero trovare sulla retta complessa descritta dall'equazione $s : \frac{1}{2} + it$. La comunità matematica, in ampia parte, ritiene che la congettura di Riemann sia vera, ma vi sono state alcune autorevoli eccezioni, come J. E. Littlewood e Atle Selberg.

L'importanza dell'ottavo problema di Hilbert, che oltre all'ipotesi di Riemann pone interrogativi anche sulle stime delle distribuzioni di primi tramite il logaritmo integrale e sulle distribuzioni di ideali primi in campi, è dovuta al forte legame esistente tra la funzione zeta e i numeri primi. Una prima connessione in tal senso fu trovata da Eulero, che notò come per ogni numero reale $x > 1$ valesse la formula prodotto che porta il suo nome

$$\zeta(x) = \prod_{p \text{ primo}} \frac{1}{1 - p^{-x}}$$

ove la produttoria spazia su tutti i primi. Oggigiorno, dopo aver assistito a svariate dimostrazioni successivamente smentite, come quella di Louis de Branges de Bourcia del 1992, per quanto i calcolatori abbiano corroborato con verifiche empiriche l'enunciato dell'ipotesi, essa è ancora un problema aperto e le conseguenze, che la sua dimostrazione affermativa causerebbe, avrebbero una portata considerevole. Infatti sulla notevole difficoltà di fattorizzare un prodotto di due numeri primi grandi si basano numerosi sistemi di sicurezza telematica, in primis l'RSA; per questo motivo la risoluzione positiva della congettura di Riemann porterebbe ad abbandonare questi sistemi di sicurezza a favore di altri, come la crittografia con funzioni ellittiche modulari o la crittografia quantistica.

1.3 Sviluppi conseguenti ai problemi di Hilbert

Non v'è dubbio, come già affermato poc'anzi, che i problemi di Hilbert costituirono e costituiscono tuttora un faro nell'oceano dei problemi insoluti della matematica. Essi, infatti, indirizzarono nel periodo immediatamente successivo alla loro stesura gli sforzi di ricerca dei matematici di tutto il mondo e non si può non notare un forte collegamento, una continuità negli intenti, tra i problemi fondazionali di Hilbert e il programma strutturale di Bourbaki, che costituitosi in Francia negli anni 1934-35 aveva come obiettivo la sistemazione rigorosa di tutte le matematiche. Ma ad oggi, quanto riuscito ad Hilbert risulta essere ancora un fatto unico e irripetuto, sebbene in molti si siano interrogati sulla possibilità di replicare un tale risultato, come per esempio il logico e matematico Hao Wang.

Ma già prima, nel 1954, era stato chiesto a John von Neumann di presentare una lista di problemi aggiornata degli originali ventitrè problemi, come base per valutare i progressi compiuti dalla matematica nell'arco di mezzo secolo. Il matematico ungherese declinò l'offerta e così si dovette attendere fino al maggio del 1974, quando l'*American Mathematical Society* organizzò uno speciale simposio con il proposito di analizzare le conseguenze di ognuno dei problemi di Hilbert e le attuali frontiere della matematica. Tuttavia, la vastità dell'impresa non permise a una sola persona, com'era stato invece possibile per Hilbert, di organizzare l'evento e riuscire nell'intento originario. Per questo il lavoro preparatorio fu iniziato da J. Dieudonnè e portato a termine da Felix E. Browder nei *Proceedings of symposia in pure mathematics*[17], includendo la collaborazione di una trentina di specialisti; il frutto del simposio, che si decise infine di limitare ai soli problemi che avessero un collegamento diretto con i ventitrè originali di Hilbert, fu una nuova lista di 130 problemi suddivisi in 27 branche. È però doveroso sottolineare come questa nuova lista risultava dal lavoro di più intelletti e non più come sintesi elaborata da una mente sola, com'era invece stato per David Hilbert. In questo senso la rassegna del 1974 non replicò quella di Parigi del 1900 e per lo stesso motivo non vi sono riusciti nemmeno Sir Michael Atiyah e John Tate, quando il 24 maggio 2000, sempre a Parigi, hanno annunciato la nuova lista dei *Millennium Problems*. Ma che l'intento di quest'ultima fosse diverso da quello dei *Mathematische Probleme* lo aveva già sottolineato Sir Andrew Wiles:

> *Con i suoi problemi, Hilbert stava cercando di guidare la matematica. Noi stiamo cercando di documentare fondamentali problemi irrisolti. In matematica esistono grandi problemi - problemi importanti - fra i quali però è difficilissimo isolarne uno che colga davvero l'essenza dell'impresa.*[18]

Quindi solo Hilbert riuscì nell'intento di indicare sia le frontiere della matematica, sia dove essa fosse diretta. E per comprendere come la matematica si sia evoluta successivamente, una pietra miliare è data da [5].

Ma venendo concretamente agli sviluppi successivi dei problemi di Hilbert[19], innanzitutto la discussione del primo problema, sebbene esso si sia dimostrato essere indecidibile, è stata foriera di grandi sviluppi nella teoria degli infiniti, ampliando oltremisura quanto iniziato da Cantor. In modo analogo, la prova della compatibilità degli assiomi dell'aritmetica ha permesso un notevole progresso nel campo della logica e della metamatematica, formalizzando ambiti come la teoria delle dimostrazioni. Pure il sesto problema sull'assiomatizzazione della fisica, per quanto troppo vago per essere risolto, interessò direttamente Hilbert e diresse lo studio teorico delle nuove branche della fisica: la teoria cinetica dei gas, la teoria statistica della radiazione, la relatività generale, la meccanica quantistica e la teoria quantistica dei campi. Prosegendo in questa sequela di sviluppi, l'ottavo problema rappresenta forse l'esempio più chiaro; infatti l'ipotesi di Riemann trova molteplici applicazioni: dalle ben note e dirette alla teoria dei numeri (e conseguentemente alla crittografia) ad altre più particolari, come le curve su campi finiti. Così, mentre particolari problemi nelle equazioni diofantee sono stati risolti in tempi relativamente recenti, come l'ultimo teorema di Fermat, altri problemi di Hilbert hanno generato a loro volta nuovi dilemmi: è

[17] Felix E. Browder, *Mathematical developments arising from Hilbert problems*, Proceedings of symposia in pure mathematics Vol. XXVIII, American Mathematical Society, Providence (Rhode Island) (1976)

[18] Keith Devlin, *I problemi del millennio*, Longanesi

[19] Per i risultati illustrati nel seguito si faccia riferimento a [5].

il caso dello *Jugendtraum* di Kronecker. Infine, passi da gigante sono stati compiuti nel provare l'esistenza di soluzioni per problemi con condizioni al contorno e nello sviluppo di nuovi metodi variazionali, per esempio per soluzioni deboli di equazioni ellittiche e per il problema di Plateau.

Sembra dunque che l'eredità lasciata da Hilbert ai posteri attraverso il suo discorso di apertura per il Secondo Congresso Internazionale dei Matematici non sia un semplice testo, ma un vero e proprio virgulto, che è attecchito sul terreno fertile di inizio Novecento e negli anni è germogliato e fiorito, producendo nuove spore e rafforzando le proprie radici, levando sempre più le sue foglie al sole.

Capitolo 2

Gruppi topologici

Much of the work of Lie and of many of his followers was on the theory in the small...
Deane Montgomery

2.1 Definizioni

Si inizi con il definire i concetti di base che saranno poi ricorrenti nelle pagine seguenti, a partire da quelli che dovrebbero essere noti fin dal primo anno di Matematica.[1]

Definizione 2.1.1. *Un gruppo è una coppia ordinata $(G, \cdot)$ ove G è un insieme e $\cdot : G \times G \to G$ è un'operazione binaria interna, detta* moltiplicazione*, tale che valgano le seguenti proprietà:*

1. *$\forall\, g_1, g_2, g_3 \in G$, $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$ (associatività);*
2. *$\exists\, e \in G$ tale che $\forall\, g \in G$, $g \cdot e = e \cdot g = g$ (esistenza dell'elemento neutro);*
3. *$\forall\, g \in G$, $\exists\, g^{-1} \in G$ tale che $g \cdot g^{-1} = g^{-1} \cdot g = e$ (esistenza dell'elemento inverso).*

Queste condizioni non sono chiaramente minime, perché, come mostrato in [8], è per esempio sufficiente richiedere l'associatività dell'operazione e l'esistenza di elementi neutro e inverso solo a sinistra, in quanto si può mostrare che questi agiscono come ci si può attendere anche a destra. Quando l'operazione di gruppo è $\cdot$, la notazione utilizzata è detta *moltiplicativa* e in tal caso, se non vi saranno ambiguità, $\cdot$ sarà omesso. Se invece l'operazione è indicata con $+$, allora il gruppo è *additivo*. Nel seguito, con lieve abuso di notazione e se ciò non sarà fonte di fraintendimenti, l'insieme G denoterà il gruppo stesso, trascurando quindi l'operazione. Si ricordi inoltre rapidamente cos'è uno spazio topologico.

[1] In questo capitolo si è fatto prevalentemente ricorso all'articolo [6] di Montgomery per quanto concerne le prime due sezioni, ma ci si è in parte basati anche su [7] per la seconda Ulteriori riferimenti sono specificati.

Definizione 2.1.2. *Uno spazio topologico è una coppia ordinata* (X, τ) *ove* X *è un insieme e* $\tau \subset \mathcal{P}(X)$ *è una famiglia di sottoinsiemi di* X *che soddisfa le seguenti richieste:*

1. $\emptyset$, $X \in \tau$;
2. $\{A_i\}_{i \in I} \subset \tau \Rightarrow \bigcup_{i \in I} A_i \in \tau$ *ove* I *è un insieme di indici;*
3. $\{A_1, ..., A_n\} \subset \tau$ *per* $n \in \mathbb{N} \Rightarrow \bigcap_{i=1}^n A_i \in \tau$.

Ora, questi concetti possono essere unificati in quello di *gruppo topologico*, che fu alla base degli sviluppi della teoria di Lie e che, pertanto, risulta fondamentale anche in questo ambito.

Definizione 2.1.3. *Un insieme* G *si dice gruppo topologico se, opportunamente equipaggiato con operazione di gruppo e topologia, risulta essere sia un gruppo che uno spazio topologico e in più le operazioni di gruppo di moltiplicazione* $(g_1, g_2) \to g_1 g_2$ *e inverso* $g \to g^{-1}$ *sono continue rispetto alla topologia assegnata.*

Evidentemente è l'ultima condizione che lega i concetti di gruppo e spazio topologico, che altrimenti sarebbero totalmente indipendenti, in quello di gruppo topologico. Si può in più osservare che la continuità delle operazioni di gruppo può essere equivalentemente riformulata come segue: se $a, b \in G$, allora per ogni intorno W di ab esistono intorni U e V di a e b rispettivamente tali che $UV \subset W$ e per ogni intorno T di a^{-1} esiste un intorno S di a tale che $S^{-1} \subset T$ [2].

Definizione 2.1.4. *Un gruppo topologico è detto essere* compatto *se, in quanto spazio topologico, risulta essere compatto e di Hausdorff.*

Definizione 2.1.5. *Un gruppo topologico si dice* localmente compatto *se, in quanto spazio topologico, risulta essere di Hausdorff e l'identità possiede un intorno compatto.*

Si osservi che se G è un gruppo topologico e H è un sottogruppo di G, allora H è anche un gruppo topologico rispetto alla topologia indotta. Così, se H è un sottospazio compatto di G, allora è anche un gruppo compatto. Ma questo sarà ribadito anche nel seguito.

2.2 Alcuni esempi significativi

In [6], Montgomery riporta alcuni esempi di gruppi topologici, in un crescendo di interesse speculativo; a questa lista si sono aggiunti alcuni esempi banali ma ugualmente significativi estratti da [7].

[2] Se A, B sono sottoinsiemi del gruppo G e $a \in G$, allora nel seguito potranno essere ricorrenti le seguenti notazioni: $AB := \{ab \,|\, a \in A, b \in B\}$, $A^{-1} := \{a^{-1} \,|\, a \in A\}$, $aB := \{ab \,|\, b \in B\}$.

Esempio 2.2.1. I numeri reali $\mathbb{R}$ formano un gruppo rispetto all'operazione di addizione, ma anche uno spazio topologico se dotati dell'usuale topologia euclidea. Poiché le operazioni di gruppo sono evidentemente continue, allora $\mathbb{R}$ forma un gruppo topologico di Hausdorff che non è compatto. Anche il gruppo moltiplicativo $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$ con la topologia indotta da quella euclidea di $\mathbb{R}$ è un gruppo topologico di Hausdorff rispetto alla moltiplicazione; il sottogruppo $\mathbb{S}^0 := \{1, -1\}$ è palesemente discreto e quindi compatto.

Esempio 2.2.2. Tutti i gruppi finiti sono gruppi topologici compatti rispetto a qualunque topologia, perché in particolare lo sono rispetto a quella discreta.

Esempio 2.2.3. I numeri complessi $\mathbb{C}$ possono essere rappresentati come punti di un piano e in tal caso, se $\mathbb{C}$ viene dotato dell'operazione di somma per componenti $(x, y) + (x', y') = (x + x', y + y')$ e della topologia del piano, in quanto $\mathbb{C} \cong \mathbb{R}^2$, allora quanto si ottiene è un altro esempio di gruppo topologico, perché le operazioni di gruppo sono chiaramente continue.
Vi è però un modo meno triviale per rendere $\mathbb{C}$ un gruppo, e in particolare un gruppo topologico; si deve definire la seguente operazione:

$$(x, y) \cdot (x', y') = (x + x'e^{-y}, y + y')$$

Evidentemente essa rende $\mathbb{C}$ un gruppo, poiché l'associatività segue da quella di somma e prodotto sui reali, l'elemento neutro è banalmente $(0, 0)$, mentre l'elemento inverso di (x, y) è $(-xe^y, -y)$. Inoltre, con questa operazione $\mathbb{C}$ è anche un gruppo topologico perché le operazioni di gruppo sono continue in quanto continue nelle loro componenti: è infatti sufficiente vedere il prodotto come una funzione $* \cdot * : \mathbb{R}^4 \to \mathbb{R}^2$ e l'inverso come $*^{-1} : \mathbb{R}^2 \to \mathbb{R}^2$. Si osservi però che in questo modo i numeri complessi vengono a costituire un gruppo non abeliano, dunque un gruppo essenzialmente differente da quello ottenuto poc'anzi rispetto alla somma; ciononostante, lo spazio topologico soggiacente è sempre lo stesso.

Esempio 2.2.4. Il gruppo moltiplicativo $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$ con l'usuale prodotto complesso è un gruppo topologico rispetto alla topologia indotta del piano. Il suo sottogruppo $\mathbb{S}^1 := \{z \in \mathbb{C} \mid |z| = 1\}$, che si visualizza geometricamente come la circonferenza complessa di raggio unitario, è un gruppo compatto, anche detto *gruppo circolare*; esso è in più isomorfo al gruppo additivo $\mathbb{R}/\mathbb{Z}$.

Esempio 2.2.5. Analogamente a quanto visto per il piano complesso, anche il gruppo moltiplicativo $\mathbb{H}^* := \mathbb{H} \setminus \{0\}$ dei quaternioni non nulli con la topologia indotta forma un gruppo topologico. Così, il sottogruppo $\mathbb{S}^3 := \{q \in \mathbb{H} \mid |q| = 1\}$ dei quaternioni unitari è compatto in $\mathbb{H}^*$.

Esempio 2.2.6. Sia $G := \{M \in \mathcal{M}(n \times n, \mathbb{R}) \mid \det M \neq 0\}$ l'insieme di tutte le matrici reali a determinante non nullo, dunque invertibili. Esso diviene un gruppo rispetto all'usuale prodotto tra matrici, meglio noto in letteratura come *gruppo lineare generale* reale di ordine n, anche indicato con $GL(n, \mathbb{R})$. Poiché ogni matrice in tale insieme può essere vista come un punto in uno spazio n^2-dimensionale, considerando banalmente gli ingressi della prima colonna come

le prime n coordinate, quelli della seconda come le successive n coordinate e avanti così, allora, dotando $\mathbb{R}^{n^2}$ della topologia euclidea, G diviene uno spazio topologico rispetto alla topologia indotta.
D'altra parte, gli ingressi di una matrice ottenuta come prodotto di altre due non sono altro che polinomi omogenei di secondo grado negli elementi delle due matrici moltiplicate; dunque, l'operazione di prodotto definita su G è continua e lo stesso può dirsi per l'operazione di inverso. Ciò significa che $GL(n, \mathbb{R})$ è un gruppo topologico; ovviamente, lo stesso discorso è valido se al posto di $\mathbb{R}$ si considera $\mathbb{C}$. Poiché ogni sottogruppo di un gruppo topologico, come osservato preliminarmente nella precedente sezione, è a sua volta un gruppo topologico, allora tutti i gruppi noti di matrici che sono sottogruppi di $GL(n, \mathbb{R})$ sono gruppi topologici. Questa osservazione si applica per esempio al gruppo ortogonale $O(n, \mathbb{R}) := \{M \in \mathcal{M}(n \times n, \mathbb{R}) \,|\, MM^t = I\}$; dalla condizione algebrica che lo determina, si può osservare che l'insieme di punti corrispondenti in $\mathbb{R}^{n^2}$ è chiuso e limitato e quindi lo spazio topologico soggiacente a tale gruppo è compatto. Tale asserzione è vera perché $O(n, \mathbb{R})$ è il luogo di zeri della funzione $MM^t - I$ e in più, considerando la norma matriciale euclidea, la richiesta $MM^t = I$ determina a sua volta la condizione $||M||^2 = \sqrt{n}$, che descrive un sottoinsieme limitato di $\mathbb{R}^{n^2}$.
Quanto visto per le matrici ortogonali è chiaramente vero anche per le matrici unitarie.

Quest'ultimo esempio può essere trattato con maggior generalità considerando uno spazio di Hilbert $\mathcal{H}$ su un campo $\mathbb{K}$ e con prodotto scalare associato $\langle \cdot, \cdot \rangle$. In tal caso il gruppo unitario su $\mathcal{H}$ è definito come $U(\mathbb{K}) := \{M : \mathcal{H} \to \mathcal{H} \,|\, \langle Mx, Mx \rangle = \langle x, x \rangle, \forall\, x \in \mathcal{H}\}$ e si può osservare facilmente che questa definizione è del tutto equivalente alla precedente. Volgendo al termine di questa collezione sufficientemente ricca di gruppi topologici, si introducano alcune utili definizioni per poter trattare in modo non banale l'ultimo esempio e comprenderlo a fondo.

Definizione 2.2.1. *Un morfismo di gruppi topologici è una funzione continua $f : G \to H$ tra i gruppi topologici menzionati che è anche un omomorfismo di gruppi. Essa è detta essere un isomorfismo di gruppi topologici se ammette un morfismo inverso; in tal caso, G e H sono detti isomorfi come gruppi topologici e si scrive $G \cong H$.*

Definizione 2.2.2. *Sia J un insieme diretto.*[3] *Un sistema proiettivo di gruppi topologici su J è una famiglia di morfismi $\mathcal{P} = \{f_{jk} : G_k \to G_j \,|\, (j, k) \in J \times J,\, j \leq k\}$, dove G_j è un gruppo topologico per ogni $j \in J$, che soddisfa le seguenti proprietà:*

(1) $\forall\, j \in J$, $f_{jj} = \mathrm{id}_{G_j}$;

[3] Un insieme diretto è una coppia ordinata $(J, \leq)$ che sarà più semplicemente indicata con J, ove $\leq$ è una relazione riflessiva e transitiva tale che ogni sottoinsieme finito non vuoto di J ha un maggiorante. Questo significa che se $\emptyset \neq K \subset J$, allora esiste un certo $j \in J$ tale che $k \leq j$ per ogni $k \in K$. Si corregga quindi la definizione data in [7], ove in più si richiede che la relazione $\leq$ sia antisimmetrica.

(2) $\forall\, j,k,l \in J$ tali che $j \leq k \leq l$, allora $f_{jk} \circ f_{kl} = f_{jl}$.

Definizione 2.2.3. *Sia $\mathcal{P}$ un sistema proiettivo di gruppi topologici e si definiscano i seguenti gruppi*

$$P := \prod_{j\in J} G_j$$

$$G := \{(g_j)_{j\in J} \in P \,|\, \forall\, j,k \in J,\ se\ j \leq k,\ allora\ f_{jk}(g_k) = g_j\}$$

ove il prodotto tra gruppi è definito come di consueto e quindi con le operazioni componente per componente.[4] *Allora il gruppo G è detto essere il limite proiettivo di $\mathcal{P}$ e può essere indicato come* $\lim_{\leftarrow} \mathcal{P}$ *oppure* $\lim_{\leftarrow j\in J} G_j$, *perché è anche noto in letteratura come* limite inverso.

Si può provare che G è un sottogruppo chiuso di P e che se tutti i gruppi G_j del sistema proiettivo sono compatti, allora lo sono anche P e G per il teorema di Tychonoff. Ovviamente, la topologia posta su P e G al fine di renderli gruppi topologici e quindi rendere continue le operazioni di gruppo è quella prodotto.

Esempio 2.2.7. Sia $\mathcal{P} = \{C_k\}_{k\in\mathbb{N}_{\geq 1}}$ una successione di gruppi topologici, ove ogni C_k denota il gruppo circolare $\mathbb{S}^1$ già incontrato nell'Esempio 2.2.4. Gli elementi di tale gruppo possono essere individuati in modo univoco in termini di un angolo misurato rispetto a un semiasse fissato. Sia altresì $\{f_k\}_{k\in\mathbb{N}_{\geq 1}}$ una successione di morfismi, ove $f_k : G_{k+1} \to G_k$ è definito semplicemente raddoppiando tale angolo: un tale omomorfismo è evidentemente due a uno. Allora l'insieme G di tutte le successioni infinite $(c_1, c_2, c_3, \dots)$, in cui $c_i = f_i(c_{i+1})$, rispetto al prodotto ottenuto dal prodotto infinito dei gruppi compatti C_k, è il limite proiettivo di $\mathcal{P}$ perché verifica la definizione fornita. Infatti è chiaro che l'operazione definita è effettivamente interna e rende G un gruppo, poiché è sufficiente sfruttare il fatto che le mappe f_k sono omomorfismi di gruppo. Per mostrare invece che G è anche un gruppo topologico, si deve esibire una topologia; sia dunque k un intero e si indichi con O_k un qualsiasi sottoinsieme aperto di C_k. Allora si definisce $(O_k)^* := \{(c_1, c_2, c_3, \dots) \in G \,|\, c_k \in O_k\}$ e tale insieme sarà detto aperto in G. La collezione $\mathcal{B}$ degli insiemi $(O_k)^*$ che possono essere costruiti nel modo appena delineato forma certamente una prebase per una topologia su G; si proverà ora che essa è in più una base.[5]

(1) banale;

[4] Se $(c_1, c_2, c_3, \dots), (c_1', c_2', c_3', \dots) \in G$, allora $(c_1, c_2, c_3, \dots) \cdot (c_1', c_2', c_3', \dots) = (c_1c_1', c_2c_2', c_3c_3', \dots)$, dove il prodotto nelle singole componenti è il prodotto definito sui rispettivi gruppi G_j.

[5] Si ricordi a tal fine il teorema di caratterizzazione delle basi. Esso afferma che dati un insieme X e una famiglia di suoi sottoinsiemi $\mathcal{B}$, $\mathcal{B}$ è una base per una topologia su X se e solo se:

1. $\forall x \in X\, \exists B \in \mathcal{B} \,|\, x \in B$;
2. $\forall B_1, B_2 \in \mathcal{B}$ tale che $B_1 \cap B_2 \neq \emptyset$, se $x \in B_1 \cap B_2$, allora $\exists B_3 \in \mathcal{B}$ tale che $x \in B_3 \subset B_1 \cap B_2$.

(2) se $A_1, A_2 \in \mathcal{B}$, allora $B = A_1 \cap A_2 \in \mathcal{B}$. Infatti per costruzione A_1 è della forma $(O_{k_1})^*$ per un certo k_1 e per un certo O_{k_1} aperto in C_{k_1}; stesso discorso vale per A_2. Sia dunque $\bar{k}$ un maggiorante per k_1 e k_2, che esiste perché l'insieme degli indici è diretto; allora, poiché le mappe f_k sono continue, le controimmagini degli aperti O_{k_1} e O_{k_2} sono aperte anch'esse in $C_{\bar{k}}$ e così pure la loro intersezione. Notando infine che in generale $(O_k)^* = (f_k^{-1}(O_k))^*$, allora $B = (\bigcap_{i=1}^2 f_{k_i\bar{k}}^{-1}(O_i))^* \in \tau$, ove $f_{k_i\bar{k}}$ è come nella Definizione 2.2.2 ed è quindi dato, molto intuitivamente, dalla composizione dei morfismi di gruppo da $f_{\bar{k}}$ fino a f_{k_i+1}.

In letteratura, lo spazio così costruito è anche noto come *solenoide*.

2.3 Proprietà dei gruppi topologici

I risultati che saranno ora riportati possono essere reperiti in [6], [7] e [9], mentre le dimostrazioni degli enunciati, alcune solo abbozzate, sono tratte da [8]. Innanzitutto, dato un qualsiasi gruppo G e un suo elemento g, è possibile definire le due seguenti mappe

$$L_g : G \to G, \qquad L_g(h) := g^{-1}h \tag{2.3.1}$$

$$R_g : G \to G, \qquad R_g(h) := hg \tag{2.3.2}$$

che sono rispettivamente dette *traslazione a sinistra* e *traslazione a destra*. Si può facilmente osservare che $L_{gh} = L_h \circ L_g$ e $L_{g^{-1}} = (L_g)^{-1}$; relazioni analoghe valgono per R_g. Inoltre, poiché nella situazione in esame G è un gruppo topologico, allora si può dire qualcosa in più: L_g e R_g sono omeomorfismi di G in se stesso. Lo stesso dicasi per l'applicazione inversa $\phi(x) := x^{-1}$.

Se si considerano due elementi qualsiasi b e c di G e si definisce $a = bc^{-1}$, allora $L_a(b) = c$: questo significa che per ogni due elementi b e c di G esiste un omeomorfismo di G in se stesso che mappa b in c [6]. Di conseguenza gli intorni di due punti qualsiasi devono essere topologicamente gli stessi, ma è chiaro che questo impone una drastica restrizione agli spazi che possono essere trasformati in un gruppo topologico: per esempio questo non può accadere per un intervallo chiuso, in quanto gli intorni dei punti di frontiera non sono omeomorfi agli intorni dei punti interni. Ancora, un fatto ulteriore che permette di decidere se un insieme può diventare un gruppo topologico, se opportunamente equipaggiato, è il seguente: se a non è l'identità di G, allora L_a non ha punti fissi e se G è connesso per archi, allora L_a è una deformazione; ma vi sono spazi che non ammettono deformazioni senza punti fissi e perciò non possono essere gruppi topologici. Per esempio solo le sfere di dimensione 1 e 3 possono essere portatrici di una struttura di gruppo. In conclusione si può mostrare (ma non sarà fatto) che le uniche varietà topologiche (in particolare connesse) di dimensione 1 o 2 cui si può dare struttura di gruppo sono la circonferenza, la retta, il piano, il

[6] In tal caso si dice che il gruppo G è omogeneo ed ogni gruppo topologico, per quanto detto, lo è.

cilindro e il toro. Volendo ora essere più dettagliati, oltre a quanto già detto, per i gruppi topologici sono inoltre verificate le seguenti proprietà:

(1) Siano $a_1, ..., a_n \in G$ e siano $r_1, ..., r_n \in \mathbb{N}$ tali che $a_1^{r_1}...a_n^{r_n} = c$. Allora per ogni intorno W di c esistono intorni $U_1, ..., U_n$ di $a_1, ..., a_n$ rispettivamente tali che $U_1^{r_1}...U_n^{r_n} \subset W$.

(2) Siano F un insieme chiuso, U un insieme aperto, P un insieme arbitrario e $a \in G$ un elemento qualsiasi, allora Fa, aF e F^{-1} sono insiemi chiusi, mentre UP, PU e U^{-1} sono insiemi aperti. Ciò segue immediatamente dal fatto che L e R sono omeomorfismi e dunque $R_a(F) = Fa$ è chiuso, così come $R_a(U) = Ua$ è aperto e dunque anche UP in quanto unione di aperti.

(3) Poiché ogni gruppo topologico G è omogeneo, allora, come già detto poc'anzi, è sufficiente controllare le proprietà locali per un singolo punto (solitamente questo viene fatto per l'elemento neutro del gruppo); in particolare la topologia è caratterizzata completamente dal sistema fondamentale di intorni di un punto.

(4) G, in quanto spazio topologico, è completamente regolare[7].

(5) Per il fatto che $\phi(x) = x^{-1}$ è continua, allora U è un intorno dell'unità e se e solo se U^{-1} lo è e in tal caso lo è anche $U \cap U^{-1}$. In più gli intorni simmetrici di e, ovvero quelli per cui $U = U^{-1}$, formano un sistema fondamentale di intorni di e, in quanto $U \cap U^{-1} \subset U$.

(6) Siano $g \in G$ e U un intorno di g, allora esiste un intorno V di e tale che $VgV \subset U$; segue immediatamente dal fatto che la moltiplicazione $G \times \{g\} \times G \to G$ per g fissato è continua nel punto (e, g, e). Di conseguenza per ogni intorno U dell'unità esiste un secondo intorno V della medesima tale che $V^2 \subset U$. Ma tale risultato si può generalizzare a un intero qualsiasi, cioè per ogni intorno U di e e per ogni $n \in \mathbb{N}$ esiste un altro intorno V di e tale che $V^n \subset U$.

(7) La mappa $f_s(x) = sxs^{-1}$ per $s \in G$ è un omeomorfismo in quanto composizione delle traslazioni L_s e R_s; poiché $f_s(e) = e$, allora segue che U è un intorno dell'unità se e solo se sUs^{-1} lo è.

(8) Un gruppo topologico G è di Hausdorff se e solo se $\{e\}$ è chiuso in G. Infatti se G è di Hausdorff, allora banalmente tutti i punti sono chiusi. Viceversa, se $\{e\}$ è chiuso, allora il complementare è aperto; pertanto per ogni $a \neq b$, da cui segue in particolare che $ab^{-1} \neq e$, esiste un intorno U

[7] Sia X uno spazio toplogico; esso è detto essere *regolare* se per ogni $a \in X$ e per ogni $B \subset X$ chiuso tale che $a \notin B$ esistono due insiemi aperti disgiunti G e H tali che $a \in G$, $B \subset H$. Esso è in più *completamente regolare* se per ogni $a \in X$ e ogni suo intorno aperto U esiste una funzione continua $f : X \to [0, 1]$ tale che $f(a) = 0$ e $f(x) = 1$ per $x \in X \setminus U$. Comunemente, questo si esprime dicendo che a e U^c possono essere separati da una funzione continua.

di e tale che $e \notin Uab^{-1}$. A questo punto non resta che considerare un secondo intorno V dell'unità tale che $V^2 \subset U$; in questo modo Va e Vb^{-1} sono intorni aperti disgiunti di a e b rispettivamente.

(9) Sia $H \subset G$ un sottogruppo di G, allora, se equipaggiato con la topologia indotta, esso diventa un gruppo topologico; in più $\overline{H}$ è un sottogruppo chiuso.

(10) Se $P, Q \subset G$ sono sottoinsiemi compatti del gruppo topologico G, allora il loro prodotto PQ è pure compatto. Infatti si mostra facilmente che la mappa prodotto $P \times Q \to PQ$ è continua e poiché il dominio è uno spazio compatto, allora lo deve essere anche la sua immagine via ogni funzione continua.

Per la trattazione successiva potrebbe essere sufficiente assumere la seguente proprietà di separazione:

$$\forall\, g_1, g_2 \in G, g_1 \neq g_2,\ \exists U \in \tau \,|\, g_1 \in U,\ g_2 \notin U,$$

la quale implica che lo spazio topologico in considerazione è di Hausdorff;[8] infatti se $g_2 = e$, allora ogni altro punto del gruppo può essere separato dall'identità, così che $\{e\}$ risulta chiuso e si ha la conclusione per la precedente proprietà (8). Non è allora particolarmente vincolante richiedere direttamente che G sia di Hausdorff, in quanto se non lo fosse, sarebbe allora sufficiente considerare il quoziente $G/\{\overline{e}\}$. Per questo motivo d'ora in poi G sarà assunto essere di Hausdorff. Per concludere, si osservi che valgono i seguenti risultati.

Proposizione 2.3.1. *Sia $A \subset G$. Allora la chiusura di A può essere caratterizzata nel seguente modo:*

$$\overline{A} = \bigcap_{V \ni e} AV = \bigcap_{V \ni e} VA$$

ove gli insiemi su cui viene presa l'intersezione sono aperti.

Proposizione 2.3.2. *Sia G un gruppo compatto. Allora ogni intorno U dell'unità contiene un secondo intorno V di e che è invariante per coniugio.*[9]

Dimostrazione. Si consideri il coniugio φ e sia U un intorno aperto dell'unità, allora $G \setminus U$ è chiaramente compatto e $W := \varphi(G \times (G \setminus U))$ è pure compatto; di conseguenza il suo complementare V è aperto, ma in più contiene l'unità, è contenuto in U ed è invariante per coniugio. Infatti

[8] Si osservi che la suddetta proprietà non deve essere confusa con l'assioma di separazione T_0, il quale invece afferma che

$$\forall\, g_1, g_2 \in G, g_1 \neq g_2,\ \exists U \in \tau \,|\, (g_1 \in U,\ g_2 \notin U) \text{ oppure } (g_1 \notin U, g_2 \in U)$$

[9] Si ricordi che l'operazione di coniugio in un gruppo è definita come di seguito:

$$\varphi : G \times G \to G, \quad \varphi(g, k) := gkg^{-1}$$

(1) se $e \in W$, allora esistono $g \in G$ e $k \in G \setminus U$ tali che $gkg^{-1} = e$, ovvero $gk = g$; ma ciò significherebbe che $k = e$, il che è però palesemente impossibile, visto che $e \notin G \setminus U$. Quindi $e \in V$.

(2) per mostrare che $V \subset U$ si può equivalentemente provare che $U^c \subset W$ e a tal fine è sufficiente osservare che $W = \varphi(G \times U^c)$ e quindi $U^c = \varphi(\{e\} \times U^c) \subset W$.

(3) per l'invarianza di V sotto coniugio e quindi per mostrare che $gVg^{-1} = V$ [10] per ogni $g \in G$ si controllino le Proposizioni 1.8 e 1.9 di [9].

Si ha perciò la conclusione. □

Si osservi inoltre che se un sottoinsieme di G è invariante per coniugio, allora anche il suo complementare lo è e lo si può dimostrare facilmente procedendo per assurdo.

[10] Si osservi che se V fosse in più un sottogruppo di G (sebbene questo non sia necessario), allora la proprietà di invarianza si tradurrebbe molto facilmente nel fatto che V è normale in G.

Capitolo 3

La misura e l'integrale di Haar

Thus there arises the question of the existence
of non-trivial linear representations.
Lev S. Pontryagin

Dopo aver così analizzato il *substratum* basilare per trattare il quinto problema di Hilbert, è ora necessario ricorrere a uno strumento in particolare, introdotto da Haar nel 1932: la misura, o equivalentemente l'integrale, che porta il suo nome. Infatti, seguendo la via intrapresa da von Neumann, si vede che per collegare un generico gruppo topologico a un più concreto gruppo di Lie (che è più direttamente investigabile e trova applicazione più specifica), se si è nel caso compatto si possono sfruttare le rappresentazioni lineari, che permettono di ricondurre i gruppi studiati a speciali gruppi di matrici.

Definizione 3.0.1. *Sia G un gruppo topologico. Una* rappresentazione lineare *di G è un omomorfismo $\phi : G \to GL(n)$ per qualche $n \in \mathbb{N}$, che è anche un morfismo di gruppi topologici, ove $GL(n)$ è il gruppo lineare generale di ordine n.*

Banalmente, ogni gruppo ammette una rappresentazione lineare banale, data dall'omomorfismo nullo che ad ogni elemento del gruppo associa la matrice identica. Per questo è sensato indagare l'esistenza di rappresentazioni lineari non triviali e si può anche procedere oltre, studiando l'eventuale esistenza di *sistemi adeguati di rappresentazioni lineari.*

Definizione 3.0.2. *Sia G un gruppo topologico. Esso ammette un* sistema adeguato di rappresentazioni lineari *se $\forall\, g \in G$ con $g \neq e$ esiste una rappresentazione lineare ϕ di G tale che $\phi(g) \neq I$, ove I è la matrice identica.*

L'esistenza di sistemi adeguati di rappresentazioni lineari per un gruppo topologico localmente compatto, in generale, non è garantita, ma è invece certa se il gruppo è compatto ed è alla dimostrazione di questo risultato che sono finalizzati questo capitolo e il seguente.

3.1 Complementi sulle funzioni continue

Poiché i gruppi topologici sono in particolare spazi topologici, allora è del tutto lecito considerare funzioni continue definite su di essi; ma la trattazione può essere affrontata in un modo leggermente differente dall'usuale, proprio per il fatto che ci si può basare sulle proprietà di gruppo e riformulare quindi concetti ben noti in tali termini.

Definizione 3.1.1. *Sia G un gruppo topologico, sia $A \subset G$ un sottoinsieme qualsiasi e sia $g \in A$; una funzione $f : A \to \mathbb{R}$ è detta essere* continua in g *se per ogni $\varepsilon > 0$ esiste un intorno V dell'unità tale che per ogni $x \in A$*

$$xg^{-1} \in V \Rightarrow |f(x) - f(g)| < \varepsilon$$

Tale definizione è equivalente a quella usuale: è infatti sufficiente osservare che $xg^{-1} \in V$ se e solo se $x \in Vg$, che è un intorno del punto g. Così si può pure parlare di uniforme continuità, prestando sufficiente attenzione.

Definizione 3.1.2 (1° formulazione)**.** *Nello scenario della precedente definizione, la funzione f è detta essere* uniformemente continua *se per ogni $\varepsilon > 0$ esiste un intorno V dell'unità tale che per ogni $x, y \in A$*

$$xy^{-1} \in V \Rightarrow |f(x) - f(y)| < \varepsilon$$

Definizione 3.1.3 (2° formulazione)**.** *Nello scenario della precedente definizione, la funzione f è detta essere* uniformemente continua *se per ogni $\varepsilon > 0$ esiste un intorno V' dell'unità tale che per ogni $x, y \in A$*

$$x^{-1}y \in V' \Rightarrow |f(x) - f(y)| < \varepsilon$$

Le due definizioni, per quanto analoghe, non sono però equivalenti, a meno che il dominio di f non sia compatto. Ma al di là della prova di questa equivalenza, è invece più utile per lo sviluppo successivo il seguente risultato.

Proposizione 3.1.1. *Sia G un gruppo topologico, sia $A \subset G$ un sottoinsieme compatto e sia $f : A \to \mathbb{R}$ una funzione continua. Allora f è anche uniformemente continua nel senso della Definizione 3.1.2 (in realtà lo sarebbe in entrambi i sensi).*

Dimostrazione. Si fissi $\varepsilon > 0$ in modo arbitrario. Poiché f è continua, allora per ogni $g \in G$ esiste un intorno V_g dell'elemento neutro tale che se $x \in A$ e $xg^{-1} \in V_g$, allora $|f(x) - f(g)| < \frac{\varepsilon}{2}$. Per la proprietà (6) enunciata al capitolo precedente, si può considerare un secondo intorno W_g dell'unità tale che $W_g^2 \subset V_g$. Inoltre gli insiemi $W_g g$, al variare di $g \in A$, costituiscono un ricoprimento di A, che, essendo compatto, ammette un sottoricoprimento finito, cioè esiste un sistema finito di elementi $g_1, ..., g_n \in A$ tale che $\bigcup_{i=1}^n W_{g_i} g_i = A$. Si indichi ora con V l'intersezione degli aperti W_{g_i}: si proverà che se $x \in A, xy^{-1} \in V$, allora $|f(x) - f(y)| < \varepsilon$, il che significa esattamente che f è uniformemente continua nel senso della prima definizione. A tal fine si osservi che, poiché gli insiemi

$W_{g_i}g_i$ ricoprono A, per ogni $y \in A$ esiste un certo k tale che $yg_k^{-1} \in W_{g_k}$ e di conseguenza $|f(y) - f(g_k)| < \frac{\varepsilon}{2}$. Per concludere non resta che osservare che

$$x \in A,\, xy^{-1} \in V \;\Rightarrow\; xg_k^{-1} = xy^{-1}yg_k^{-1} \in VW_{g_k} \subset W_{g_k}^2 \subset V_{g_k}$$

e quindi anche $|f(x) - f(g_k)| < \frac{\varepsilon}{2}$. Di conseguenza, per disuguaglianza triangolare, $|f(x) - f(y)| < \varepsilon$, provando così l'enunciato.

$\square$

In modo esattamente analogo all'Analisi classica, anche in questo contesto si può parlare di famiglie di funzioni equicontinue ed equilimitate e, visto che la convergenza uniforme si definisce in questo ambito senza variazioni di sorta, allora è valido il ben noto teorema di Ascoli-Arzelà, di cui si ricorda l'enunciato e la cui dimostrazione può essere condotta per i gruppi in modo sostanzialmente canonico.

Teorema 3.1.1 (Ascoli-Arzelà)**.** *Siano G un gruppo topologico e sia $A \subset G$ un suo sottoinsieme compatto; sia inoltre $\mathcal{F}$ una famiglia equilimitata ed equicontinua di funzioni a valori reali definite su A. Sotto queste ipotesi, ogni successione contenuta in $\mathcal{F}$ ammette una sottosuccessione uniformemente convergente a una funzione continua (in particolare uniformemente continua, visto che è continua sul compatto A).*

Tralasciando per l'appunto la dimostrazione, che il lettore può trovare in [8], si compia un'ultima osservazione, non particolarmente profonda ma utile, anche nel seguito, dal punto di vista notazionale[1]. Se M è uno spazio topologico compatto e f è una funzione continua su di esso, allora per il teorema di Weierstrass f assume massimo e minimo, che saranno indicati rispettivamente con $L(f)$ e $K(f)$; inoltre si può definire l'oscillazione di f come $S(f) := L(f) - K(f)$. Se a questo punto si considera una successione di funzioni continue $\{f_n\}_{n\in\mathbb{N}}$ tale che $f_n \to f$ uniformemente su M, allora sono facilmente verificate le seguenti relazioni:

$$\lim_{n\to\infty} K(f_n) = K(f), \quad \lim_{n\to\infty} L(f_n) = L(f), \quad \lim_{n\to\infty} S(f_n) = S(f) \tag{3.1.1}$$

3.2 Il teorema di esistenza e unicità

A questo punto tutti i tasselli sono stati posizionati correttamente e si può quindi definire in primis un integrale invariante su un gruppo topologico G, dopodichè provarne esistenza e unicità[2]. Si mostrerà inoltre che alcune proprietà assunte nella definizione sono automaticamente verificate se valgono le rimanenti, con dettagli che saranno ovviamente specificati. Come ultima precisazione, in realtà sarebbe stato del tutto equivalente definire una misura invariante su un gruppo topologico G, ma si è preferito l'approccio integrale per la chiarezza della dimostrazione fornita in [8].

[1] Si ricordi che si fa riferimento a [8] per quanto riguarda le scelte notazionali.

[2] La dimostrazione che sarà seguita e presentata in [8] si basa essenzialmente sul lavoro di von Neumann.

Definizione 3.2.1. *Sia G un gruppo topologico compatto. Un* integrale invariante normalizzato[3] *è definito su G se ad ogni funzione reale continua definita su G è associato un valore reale, denotato con $\int f(x)dx$ e detto integrale di f su G, tale che sono soddisfatte le seguenti proprietà:*

1. *(omogeneità) se $\alpha \in \mathbb{R}$, allora $\int \alpha f(x)dx = \alpha \int f(x)dx$;*
2. *(additività) se f e g sono due funzioni continue, allora $\int(f(x)+g(x))dx = \int f(x)dx + \int g(x)dx$;*
3. *(monotonia) se f è ovunque non negativa, cioè $f(x) \geq 0\ \forall x \in G$, allora $\int f(x)dx \geq 0$;*
4. *(normalizzazione) se $f(x) = 1\ \forall x \in G$, allora $\int f(x)dx = 1$;*
5. *se f è ovunque non negativa e in più non identicamente nulla, allora $\int f(x)dx > 0$;*
6. *(invarianza a destra) $\forall g \in G$, $\int f(xg)dx = \int f(x)dx$;*
7. *(invarianza a sinistra) $\forall g \in G$, $\int f(gx)dx = \int f(x)dx$;*
8. *(invarianza per inversione) $\int f(x^{-1})dx = \int f(x)dx$.*

Di questi requisiti, i primi cinque (la normalizzazione si riformula come finitezza sui compatti) ricorrono per ogni concetto di integrale e sono dunque basilari, mentre i rimanenti rispecchiano la proprietà di invarianza del gruppo. Non si può non notare la forte somiglianza che lega le proprietà 6. e 7. alla ben nota invarianza per traslazioni della misura di Lebesgue su $\mathbb{R}^n$. Infatti, da quanto appreso nei corsi di Analisi Matematica dovrebbe essere consolidato il fatto che per ogni $\mathbf{y} \in \mathbb{R}^n$ e per ogni funzione f Lebesgue-misurabile a valori reali

$$\int_{\mathbb{R}^n} f(\mathbf{x}+\mathbf{y})d\mu_n = \int_{\mathbb{R}^n} f(\mathbf{x})d\mu_n$$

Così, per ogni $a \neq 0$ reale è pure verificata la seguente relazione

$$\int_{\mathbb{R}^n\setminus\{0\}} \frac{f(a\mathbf{x})}{\mathbf{x}}d\mu_n = \int_{\mathbb{R}^n\setminus\{0\}} \frac{f(\mathbf{x})}{\mathbf{x}}d\mu_n$$

Queste identità, alla luce di quanto verrà ora mostrato, non sono altro che semplici generalizzazioni dell'integrale o della misura di Haar ai gruppi topologici $(\mathbb{R}^n, +)$ e $(\mathbb{R}^n \setminus \{0\}, \cdot)$ rispettivamente. Infatti la definizione appena fornita di

[3] L'aggettivo *normalizzato*, come appare chiaro dalla proprietà 4., è giustificato dal fatto che l'integrale su G della funzione costante 1 è pari a 1, cioè la misura del gruppo è 1. Questa caratteristica può però essere imposta solo per integrali/misure definiti su gruppi compatti. Nel caso in cui si abbia a che fare con un gruppo localmente compatto, tale richiesta viene rimpiazzata imponendo che l'integrale sia finito sui compatti o che la misura dei compatti sia finita. Questo è esattamente quello che accade con la misura di Lebesgue su $\mathbb{R}^n$; poiché questa soddisfa anche tutte le altre proprietà, allora essa è, a meno di fattori di scala, la misura di Haar sul gruppo topologico $(\mathbb{R}^n, +)$.

integrale invariante è stata addomesticata agli scopi della trattazione, ovvero al caso compatto; in realtà è possibile definire l'integrale di Haar su gruppi localmente compatti, come per l'appunto $\mathbb{R}^n$ e $\mathbb{R}^n \setminus \{0\}$ con le rispettive operazioni, ma in tal caso si deve distinguere tra invarianza a destra, a sinistra e per inversioni. Al contrario nel caso compatto, come mostrato da von Neumann, le misure e gli integrali invarianti a destra lo sono anche a sinistra e viceversa. Senza addentrarsi troppo nel merito del caso localmente compatto, si riprenda la precedente discussione.

Osservazione 3.2.1. Si osservi che le prime tre condizioni della definizione di integrale invariante normalizzato permettono di ricavare due proprietà note degli integrali, cioè la monotonia e la stima in valore assoluto. Questo significa che dalle summenzionate proprietà consegue che se f, g sono funzioni continue sul gruppo compatto G e in più $f(x) \leq g(x)\ \forall x \in G$, allora

$$\int f(x)dx \leq \int g(x)dx, \qquad \left| \int f(x)dx \right| \leq \int |f(x)|dx$$

La dimostrazione è immediata.

Dimostrazione. Innanzitutto $f(x) \leq g(x)$ si può riscrivere come $g(x) - f(x) \geq 0$ e quindi per la proprietà 3. $\int (g(x) - f(x))dx \geq 0$; ma ora, per le prime due proprietà si conclude che $\int g(x)dx - \int f(x)dx \geq 0$ e questo prova quanto voluto. Così, per la seconda disuguaglianza si osservi che

$$-|f(x)| \leq f(x) \leq |f(x)| \Rightarrow -\int |f(x)|dx \leq \int f(x)dx \leq \int |f(x)|dx$$

che non è altro che $\left| \int f(x)dx \right| \leq \int |f(x)|dx$, cioè quanto si voleva provare. $\square$

A questo punto si può passare finalmente al teorema che garantisce l'esistenza e l'unicità su gruppi topologici compatti di integrali di Haar invarianti a destra, a sinistra e per inversioni.

Teorema 3.2.1. *Sia G un gruppo topologico compatto. Allora su di esso esiste ed è unico un integrale invariante. In più, se su G è dato un integrale che soddisfa le proprietà 1., 2., 3., 4. e 6., allora le rimanenti condizioni della Definizione 3.2.1 sono automaticamente verificate.*

La dimostrazione è alquanto lunga e articolata e per questo sarà suddivisa in alcune proposizioni od osservazioni ausiliarie. Nel seguito sarà inoltre sottintesa l'ipotesi che il gruppo G in considerazione è compatto.

Osservazione 3.2.2. Siano f una funzione continua definita su G e $A = \{a_1, ..., a_n\}$ un sottoinsieme finito di elementi di G, non necessariamente distinti, allora si può introdurre la funzione $M(A, f) : G \to G$ definita come segue:

$$M(A, f)(x) := \sum_{i=1}^{n} \frac{f(xa_i)}{n}$$

Si vede facilmente che essa è continua e in più dovrebbe apparire evidente che sarà alla base della costruzione dell'integrale invariante cercato; infatti nella forma è analoga alle funzioni a scala utilizzate per costruire l'integrale di Riemann e Lebesgue. Per questo motivo una funzione siffatta sarà d'ora in poi detta *semplice a destra*. Un primo fatto interessante è che per tale funzione sono soddisfatte le seguenti tre disuguaglianze

$$K(M(A,f)) \geq K(f) \tag{3.2.1}$$

$$L(M(A,f)) \leq L(f) \tag{3.2.2}$$

$$S(M(A,f)) \leq S(f) \tag{3.2.3}$$

per il semplice motivo che, per esempio,

$$K(M(A,f)) \geq \sum_{i=1}^{n} \min_{x \in G} \frac{f(xa_i)}{n} = \sum_{i=1}^{n} \min_{G} \frac{f}{n} = K(f)$$

Inoltre se $A = \{a_1, ..., a_n\}$ e $B = \{b_1, ..., b_m\}$ sono due sottoinsiemi finiti di G, allora

$$M(A, M(B,f)) = M(AB, f) \tag{3.2.4}$$

La dimostrazione è immediata e si osservi che l'identità è verificata per AB e non, in generale, per BA, nel senso che $M(AB,f) \neq M(BA,f)$.

Osservazione 3.2.3. Banalmente, per le funzioni semplici a destra valgono linearità e additività, ovvero

$$M(A, \lambda f) = \lambda M(A,f), \qquad M(A, f+g) = M(A,f) + M(A,g)$$

per ogni sottoinsieme finito $A \subset G$, avendo posto $(\lambda f)(x) := \lambda f(x)$ e $(f+g)(x) := f(x) + g(x)$.

Proposizione 3.2.1. *Sia f una funzione continua non costante definita su G; allora G contiene un sottoinsieme finito A tale che*

$$S(M(A,f)) < S(f)$$

Dimostrazione. Si indichino rispettivamente con k e l il minimo e il massimo di f; poiché f è non costante, allora $k < l$ e, dato che essa è in più continua, allora esiste un aperto $U \subset G$ tale che per ogni $x \in U$ è soddisfatta la disuguaglianza $f(x) \leq h < l$, ove $h := \frac{k+l}{2}$. In secondo luogo si osservi che la collezione $\{Ua^{-1}\}_{a \in G}$ costituisce un ricoprimento di G e quindi esiste un sottoinsieme finito $A = \{a_1, ..., a_n\}$ tale che $\bigcup_{i=1}^{n} Ua_i^{-1} = G$. A questo punto si deve mostrare che

$$\max_{x \in G} M(A,f)(x) \leq \frac{(n-1)l + h}{n} < l$$

e a tal fine è sufficiente osservare che per ogni $x \in G$, $f(xa_i) \leq l$ per ogni $i = 1, ..., n$. D'altra parte è altresì vero che per ogni $x \in G$ esiste un intero $j \in$

$\{1, ..., n\}$ tale che $x \in Ua_j^{-1}$; di conseguenza $xa_j \in U$ e quindi, per quanto detto poc'anzi, $f(xa_j) \leq h$. In questo modo la suddetta disuguaglianza è provata. Poiché per (3.2.1) il minimo di $M(A, f)$ è maggiore di quello di f, allora in conclusione

$$S(M(A, f)) = L(M(A, f)) - K(M(A, f)) < l - K(M(A, f)) \leq l - k = S(f)$$

L'enunciato è provato. $\square$

Il passo successivo è ora quello di mostrare che ogni funzione continua ammette almeno un *integrale a destra* o *destro* e a tale scopo sarà indispensabile ricorrere al teorema di Ascoli-Arzelà.

Definizione 3.2.2. *Sia $f : G \to \mathbb{R}$ una funzione continua. Il numero reale p è detto essere un* integrale destro *per f se per ogni $\varepsilon > 0$ esiste un sottoinsieme finito $A \subset G$ tale che*

$$\forall x \in G, \ |M(A, f)(x) - p| < \varepsilon \tag{3.2.5}$$

Proposizione 3.2.2. *Sia $f : G \to \mathbb{R}$ una funzione continua. Allora f ammette almeno un integrale destro.*

Dimostrazione. Sia f una funzione continua fissata e definita su G. Si indichi con $\mathcal{F}$ l'insieme di tutte le funzioni del tipo $M(A, f)$ al variare del sottoinsieme finito A di G. Per (3.2.1) e (3.2.2) è chiaro che $\mathcal{F}$ è una famiglia equilimitata di funzioni; si tratta ora di provare che è anche equicontinua.

Innanzitutto f, essendo continua sul compatto G, è anche uniformemente continua; di conseguenza, per la Definizione 3.1.2, per ogni $\varepsilon > 0$ esiste un intorno V dell'unità tale che se $xy^{-1} \in V$, allora $|f(x) - f(y)| < \varepsilon$. Ma se $xy^{-1} \in V$, allora anche $(xa_i)(ya_i)^{-1} \in V$ e quindi $|f(xa_i) - f(ya_i)| < \varepsilon$. Se ora si somma questa disuguaglianza su i e si divide il risultato per n, allora si ottiene

$$|M(A, f)(x) - M(A, f)(y)| < \varepsilon$$

A questo punto, visto che la disuguaglianza è vera per ogni $xy^{-1} \in V$ e per ogni sottoinsieme arbitrario A, allora tutte le funzioni di $\mathcal{F}$ sono limitate dallo stesso ε su V, ovvero $\mathcal{F}$ è una famiglia equicontinua. Quindi sono verificate le ipotesi del Teorema 3.1.1, che sarà tra breve applicato. Prima però si definisca

$$s := \inf_{A \subset G, \, |A| < \infty} S(M(A, f))$$

che indica l'estremo inferiore delle oscillazioni di tutte le funzioni appartenenti a $\mathcal{F}$ ed esiste certamente finito, in quanto tali funzioni sono equilimitate. Per il semplice fatto che s esiste, si può allora considerare una successione di funzioni $\{f_n\}_{n \in \mathbb{N}} \subset \mathcal{F}$ tale che

$$\lim_{n \to \infty} S(f_n) = s$$

Ma d'altra parte, per il Teorema 3.1.1, dalla successione $\{f_n\}_{n \in \mathbb{N}}$ può essere estratta una sottosuccessione $\{f_{n_j}\}$ tale che $f_{n_j} \to g$ uniformemente su G, ove

g, in quanto limite uniforme di una successione di funzioni continue, è a sua volta continua[4]. Poiché $\lim_{n\to\infty} S(f_n) = s$, allora anche $\lim_{j\to\infty} S(f_{n_j}) = s$ e poiché la convergenza di f_{n_j} a g è uniforme, allora per la terza relazione in (3.1.1) si ha che $S(g) = s$.

Ora si proverà che g è costante, o equivalentemente che $s = 0$, perché dimostrato ciò si potrà concludere rapidamente. Infatti, visto che $f_{n_j} \to g$ uniformemente, allora, posto $p := g(x)$ per ogni $x \in G$, si ha che per ogni $\varepsilon > 0$ esiste $\bar{n} \in \mathbb{N}$ tale che

$$n_j \geq \bar{n} \;\Rightarrow\; \forall\, x \in G,\, |f_{n_j}(x) - p| < \varepsilon$$

ma poiché $f_{n_j} \in \mathcal{F}$, allora esiste un certo sottoinsieme finito $A_j \subset G$ tale che $f_{n_j} = M(A_j, f)$. A questo punto è sufficiente considerare un qualsiasi intero n che verifica la suddetta disuguaglianza, sia $\bar{n}$, così che in conclusione per ogni $\varepsilon > 0$ esiste un sottoinsieme finito $A_{\bar{n}} \subset G$ tale che (3.2.5) sia verificata.

Per provare effettivamente che g è costante si proceda per assurdo. Innanzitutto, in virtù della Proposizione 3.2.1, esiste un sottoinsieme finito $A \subset G$ tale che

$$S(M(A, g)) = s' < s \tag{3.2.6}$$

Sia quindi $\varepsilon := \frac{s-s'}{3}$; poiché, come già detto, $f_{n_j} \to g$ uniformemente, allora esiste un certo indice $k \in \mathbb{N}$ tale che, di lì in poi, $|g(x) - f_{n_j}(x)| < \varepsilon$ per ogni $x \in G$. In modo analogo a quanto compiuto nella parte iniziale di questa dimostrazione, si può sostituire xa_i a x nell'ultima disuguaglianza, dove $a_i \in A$. Sommando poi le relazioni così ottenute per $i = 1, ..., n$ e dividendo per n si ricava che

$$|M(A, g)(x) - M(A, f_{n_j})(x)| < \varepsilon$$

o equivalentemente

$$|M(A, f_{n_j})(x)| < |M(A, g)(x)| + \varepsilon \tag{3.2.7}$$

A questo punto, unendo (3.2.6) e (3.2.7), si ottiene che

$$S(M(A, f_{n_j})) \leq s' + 2\varepsilon < s$$

Ma ora si osservi che, poiché $f_{n_j} \in \mathcal{F}$, allora per (3.2.4) anche $M(A, f_{n_j}) \in \mathcal{F}$ e l'assurdo è evidente: infatti l'oscillazione di $M(A, f_{n_j})$ deve essere maggiore di s. Dunque g è costante e, per quanto già detto poco sopra, consegue che $p = g(x)$ è un integrale destro per f. □

Il discorso fin qui condotto per le funzioni semplici a destra può essere riproposto *mutatis mutandis* per quelle semplici a sinistra. Si può cioè, per una funzione continua f definita su G e per un sottoinsieme finito $B = \{b_1, ..., b_m\}$ di G, definire la funzione $M'(B, f) : G \to G$ come

$$M'(B, f)(x) := \sum_{j=1}^{m} \frac{f(b_j x)}{m}$$

[4] Tuttavia non è detto che $g \in \mathcal{F}$.

Per queste nuove funzioni valgono le proprietà già viste per le semplici a destra e in più vale banalmente la relazione

$$M(A, M'(B, f)) = M'(B, M(A, f)) \tag{3.2.8}$$

Dimostrazione.

$$\begin{aligned} M(A, M'(B, f))(x) &= \sum_{i=1}^{n} \frac{M'(B, f)(xa_i)}{n} = \sum_{i=1}^{n} \sum_{j=1}^{m} \frac{f(b_j x a_i)}{mn} = \\ &= \sum_{j=1}^{m} \frac{M(A, f)(b_j x)}{m} = M'(B, M(A, f))(x) \end{aligned}$$

□

Inoltre si può introdurre la nozione di *integrale sinistro* semplicemente adattando la precedente. Pertanto il numero reale q sarà detto essere un integrale sinistro per la funzione continua f definita su G se per ogni $\varepsilon > 0$ esiste un sottoinsieme finito $B \subset G$ tale che

$$\forall x \in G,\ |M'(B, f)(x) - q| < \varepsilon \tag{3.2.9}$$

Per provare l'analogo della Proposizione 3.2.2 e quindi l'esistenza di almeno un integrale sinistro per f si può scimmiottare la dimostrazione appena conclusa oppure, più saggiamente, si può considerare un nuovo gruppo $(G', *)$, ove $G' = G$ e la topologia su G' è la stessa di G, ma è invece differente l'operazione di gruppo, data da $a * b := b \cdot a$ (in cui $\cdot$ è l'operazione di G). In questo modo G' è un gruppo topologico e un integrale destro per una funzione definita su G' è un integrale sinistro per la stessa funzione definita su G. Poiché per la Proposizione 3.2.2 l'esistenza di integrali destri è garantita, allora si può concludere che ogni funzione continua definita su G ammette sia un integrale destro, sia un integrale sinistro.

A questo punto è però lecito attendersi in più che esistano un solo integrale destro e un solo integrale sinistro e che inoltre questi coincidano.

Lemma 3.2.1. *Sia f una funzione continua definita su G. Allora essa ammette un solo integrale destro p e un solo integrale sinistro q. Inoltre $p = q$ e l'unico numero così associato a f sarà detto il suo integrale (tout court) e indicato con $M(f)$.*

Dimostrazione. Siano p e q come nell'enunciato, allora per opportune scelte di A e B le definizioni di integrale destro e integrale sinistro sono verificate, ovvero sono valide (3.2.5) e (3.2.9). Se ora in (3.2.5) si sostituisce $b_j x$ a x, si somma per $j = 1, ..., m$ e si divide il risultato per m, allora si ottiene

$$|M'(B, M(A, f))(x) - p| < \varepsilon\ \forall x \in G$$

Analogamente, in (3.2.9) si deve sostituire xa_i a x, sommare su $i = 1, ..., n$ e dividere il risultato per n, così da avere

$$M(A, M'(B, f))(x) - q| < \varepsilon\ \forall x \in G$$

In conclusione, tenendo conto di (3.2.8), è chiaro che per semplice disuguaglianza triangolare $|p - q| < 2\varepsilon$ e, visto che ε è arbitrario, allora $p = q$. □

Ora si dispone di un preciso oggetto matematico e si vedrà che esso soddisfa le otto proprietà richieste dalla Definizione 3.2.1. Ma per come è stato definito $M(f)$ dovrebbe essere evidente che 1., 3. e 4. sono immediatamente verificate. Infatti se p è un integrale per f, allora αp è un integrale per αf, poiché lo scalare può essere raccolto ed estratto in valore assoluto dal modulo in (3.2.5) e (3.2.9). Così, se f è positiva, il suo integrale non può che essere positivo, in quanto tutte le funzioni semplici (a destra e a sinistra) lo sono e infine, se $f \equiv 1$, allora anche tutte le funzioni semplici sono identicamente pari a 1; di conseguenza deve esserlo anche l'integrale di f. Si passi perciò alla dimostrazione delle rimanenti proprietà.

Proposizione 3.2.3. *Siano f, g due funzioni continua definite su G. Allora*

$$M(f + g) = M(f) + M(g)$$

Dimostrazione. Si inizi con il provare che

$$M(M(B, f)) = M(f) \tag{3.2.10}$$

per ogni sottoinsieme finito $B \subset G$. A tal fine sia $M(f) = p$; per quanto detto precedentemente, p è in particolare anche un integrale sinistro di f e quindi per ogni $\varepsilon > 0$ esiste un certo sottoinsieme finito $C \subset G$ tale che $|M'(C, f)(x) - p| < \varepsilon$. Come di consueto, se si sostituisce xb_j al posto di x e si somma la disuguaglianza per $j = 1, ..., m$, ricorrendo alla disuguaglianza triangolare si ottiene

$$|M(B, M'(C, f))(x) - p| \leq \sum_{j=1}^{m} \frac{|M'(C, f)(xb_j) - p|}{m} < \varepsilon \ \forall x \in G$$

Indi, per (3.2.8), questa relazione può essere riscritta come

$$|M'(C, M(B, f))(x) - p| < \varepsilon \ \forall x \in G$$

Ma questo significa esattamente che p è un integrale sinistro anche per $M(B, f)$, provando così (3.2.10). Sia poi $M(g) = q$; allora q è in particolare un integrale destro di g e quindi per ogni $\varepsilon > 0$ esiste un sottoinsieme finito $B \subset G$ tale che

$$|M(B, g)(x) - q| < \varepsilon \ \forall x \in G$$

Con la solita procedura, per ogni sottoinsieme finito $\tilde{A} \subset G$ vale

$$|M(\tilde{A}, M(B, g))(x) - q| < \varepsilon \ \forall x \in G$$

ma ricordando (3.2.4) si ottiene che

$$|M(\tilde{A}B, g)(x) - q| < \varepsilon \ \forall x \in G \tag{3.2.11}$$

Ora, riprendendo quanto visto all'inizio di questa dimostrazione, poiché p è anche un integrale destro di $M(B, f)$ per B arbitrario, allora per ogni $\varepsilon > 0$ esiste un sottoinsieme finito $A \subset G$ tale che

$$|M(A, M(B, f))(x) - p| < \varepsilon \ \forall x \in G$$

ma ancora, per (3.2.4), quest'ultima disuguaglianza si può riscrivere come

$$|M(AB, f)(x) - p| < \varepsilon \ \forall x \in G$$

A questo punto, visto che $\tilde{A}$ è arbitrario in (3.2.11), allora nulla vieta di poter scegliere $\tilde{A} = A$. In conclusione, per l'Osservazione 3.2.3, con quest'ultima mossa si ha che

$$|M(AB, f+g)(x) - (p+q)| \leq |M(AB, f)(x) - p| + |M(AB, g)(x) - q| < 2\varepsilon$$

e quindi si vince, perché data l'arbitrarietà di ε si può asserire che $p + q$ è un integrale destro di $f + g$. □

Dopo questo sforzo, le rimanenti proprietà si verificano molto facilmente.

Proposizione 3.2.4. *Sia f una funzione continua definita su G e sia $g \in G$ un elemento arbitrario del gruppo. Allora, posti $f_1(x) := f(xg)$ e $f_2(x) := f(gx)$, valgono le proprietà 6. e 7. della Definizione 3.2.1, cioè*

$$M(f_1) = M(f), \qquad M(f_2) = M(f)$$

Dimostrazione. È sufficiente osservare che $M(A, f_1) = M(Ag, f)$, semplicemente per la definizione di funzione semplice a destra. Ne segue immediatamente che gli integrali destri di f e f_1 coincidono, perché per ogni sottoinsieme finito $A \subset G$ che soddisfa la Definizione 3.2.2 per f, l'insieme Ag la verifica per f_1 e viceversa, se B realizza la medesima definizione per f_1, allora Bg^{-1} la verifica per f. Quindi è subito verificato che $M(f_1) = M(f)$.

Per mostrare che $M(f_2) = M(f)$, il ragionamento è analogo, ma si utilizza l'integrale sinistro al posto di quello destro. □

Proposizione 3.2.5. *Sia f una funzione continua definita su G e si definisca $\bar{f}(x) := f(x^{-1})$ per ogni $x \in G$. Allora vale la proprietà 8. della Definizione 3.2.1, cioè*

$$M(\bar{f}) = M(f)$$

Dimostrazione. Non vi è necessità di dilungarsi eccessivamente su questa dimostrazione. Infatti, se $M(f) = p$, allora per ogni $\varepsilon > 0$ esiste un sottoinsieme finito $A \subset G$ tale che $|M(A, f)(x) - p| < \varepsilon$ per ogni $x \in G$; ma è chiaro che nulla cambia affermando che la stessa disuguaglianza è vera per ogni $x^{-1} \in G$, visto che l'elemento inverso esiste per ogni elemento di G. □

Proposizione 3.2.6. *Sia f una funzione continua non negativa definita su G e non identicamente nulla, allora è soddisfatta la proprietà 5. della Definizione 3.2.1, ovvero*

$$M(f) > 0$$

Dimostrazione. Per semplice continuità di f e poiché f non è identicamente nulla, esiste un aperto $U \subset G$ tale che se $x \in U$, allora $f(x) \geq \varepsilon > 0$. Gli insiemi aperti Ug^{-1}, al variare di $g \in G$, ricoprono G e poiché quest'ultimo è compatto, allora esiste un sottoinsieme finito di punti $A = \{g_1, ..., g_n\}$ tale che gli aperti associati della forma suddetta sono un ricoprimento di G. Inoltre, per ogni $x \in G$ si ha che $f(x) \geq 0$ ed esiste un indice $k \in \{1, ..., n\}$ tale che $x \in Ug_k^{-1}$; ma ciò significa che $xg_k \in U$ e quindi $f(xg_k) \geq \varepsilon$. Di conseguenza

$$M(A, f)(x) \geq \frac{\varepsilon}{n} > 0, \ \forall x \in G$$

da cui segue che $M(f) = M(M(A, f)) \geq \frac{\varepsilon}{n} > 0$, provando quanto voluto. Si osservi in particolare che la prima uguaglianza è giustificata da (3.2.10). $\square$

Si può perciò definire l'integrale (invariante e normalizzato) di una funzione continua arbitraria definita su G come

$$\int f(x)dx := M(f)$$

in quanto si è provato che tutte le richieste sono soddisfatte. A questo punto si è pronti per concludere la dimostrazione del Teorema 3.2.1, di cui si è già provata la prima parte, che afferma l'esistenza dell'integrale di Haar. Non resta che provare che se $\int^* f(x)dx$ è un altro integrale definito su G che verifica le proprietà dalla 1. alla 4. e in più la 6., allora valgono anche le rimanenti e

$$\int^* f(x)dx = M(f) \tag{3.2.12}$$

Questo significa che solo alcune delle proprietà espresse nella Definizione 3.2.1 sono necessarie e in più l'integrale di f definito come $M(f)$ è unico.

Dimostrazione. (del Teorema 3.2.1)

Sia p un integrale destro di f, così che per ogni $\varepsilon > 0$ esiste un opportuno sottoinsieme finito $A \subset G$ tale che $|M(A, f)(x) - p| < \varepsilon$ per ogni $x \in G$. Per quanto visto nell'Osservazione 3.2.1, sono sufficienti le prime tre proprietà per integrare le disuguaglianze e quindi il seguente passaggio è del tutto lecito.

$$\left| \int^* M(A, f)(x)dx - p \right| \leq \varepsilon$$

In particolare $\int^* \varepsilon dx = 1$, poiché per 1. lo scalare può essere estratto, mentre per 4. l'integrale su G della funzione identicamente 1 è normalizzato. Ma ancora, in virtù di 6. questa relazione può essere riscritta come segue

$$\left| \int^* f(x)dx - p \right| \leq \varepsilon$$

e poiché essa è valida per ogni $\varepsilon > 0$, allora si deduce che vale (3.2.12). In questo modo l'unicità è provata e visto che $M(f)$ verifica tutte le proprietà della Definizione 3.2.1, allora questo vale anche per $\int^* f(x)dx$, concludendo la dimostrazione. $\square$

In conclusione, quanto appena visto per funzioni reali può essere esteso anche a funzioni a valori complessi $h = f + ig$, ove f, g sono funzioni a valori reali. In tal caso h è continua se e solo se f, g lo sono e il suo integrale può essere definito come

$$\int h(x)dx := \int f(x)dx + i \int g(x)dx$$

Infine l'integrale di Haar può essere esteso al prodotto diretto di gruppi topologici e in tale ambito è irrilevante l'ordine di integrazione, analogamente a quanto afferma il noto teorema di Fubini-Tonelli. Questo risultato sarà discusso nel prossimo capitolo. Ma prima di concludere, un esempio facile e immediato.

Esempio 3.2.1. Sia G un gruppo topologico finito. Allora l'integrale di qualsiasi funzione definita sul gruppo è semplicemente la media aritmetica dei valori assunti dalla funzione stessa.

3.3 Equivalenza tra approccio integrale e approccio insiemistico

Per quanto non necessario ai fini della trattazione principale, si è ugualmente deciso di spendere alcune parole sull'effettiva equivalenza di possedere un integrale di Haar anzichè una misura di Haar. Ciò sarà fatto seguendo l'esempio di [10], senza particolari pretese. Infatti si è scelto di trattare solo succintamente quanto esposto da Kelley e Srinivasan, ma per rendere comprensibili le nozioni utilizzate si deve aprire una parentesi terminologica.

Definizione 3.3.1. *Sia X uno spazio di Hausdorff localmente compatto. Una* misura *su X è una funzione $\mu : \mathcal{C} \to \mathbb{R}_+$, ove $\mathcal{C}$ è la famiglia degli insiemi compatti di X, subadditiva, additiva e monotona, ovvero*

1. *(non negatività) $\forall A \in \mathcal{C}$, $0 \leq \mu(A) < \infty$;*
2. *(subadditività) $\forall A, B \in \mathcal{C}$, $\mu(A \cup B) \leq \mu(A) + \mu(B)$;*
3. *(additività) $\forall A, B \in \mathcal{C} \,|\, A \cap B = \emptyset$, $\mu(A \cup B) = \mu(A) + \mu(B)$;*
4. *(monotonia) $\forall A, B \in \mathcal{C} \,|\, A \subset B$, $\mu(A) \leq \mu(B)$.*

Una misura μ si dice in più regolare *se per ogni $A \in \mathcal{C}$ e per ogni $\varepsilon > 0$ esiste $B \in \mathcal{C}$ tale che $\mathring{B} \supset A$ e $\mu(B) \leq \mu(A) + \varepsilon$, cioè*

$$\mu(A) = \inf\{\mu(B) \,|\, B \in \mathcal{C},\ \mathring{B} \supset A\}$$

Più in generale una misura potrebbe essere definita su un δ-anello, ovvero un anello di insiemi (sul quale si tornerà tra breve) chiuso per intersezione numerabile, ma poiché si avrà a che fare con gruppi topologici, è allora immediato constatare che $\mathcal{C}$ è precisamente un δ-anello.

Definizione 3.3.2. *Sia X uno spazio di Hausdorff localmente compatto. Una* premisura *su X è una funzione $\nu : \mathcal{B} \to \mathbb{R}_+$ subadditiva, additiva, monotona (nel senso descritto precedentemente) definita su una famiglia $\mathcal{B}$ di sottoinsiemi compatti di X che godono delle seguenti proprietà:*

1. *$\forall A, B \in \mathcal{B}$, $A \cup B \in \mathcal{B}$;*
2. *$\mathcal{B}$ è una base per gli intorni dei compatti di X, cioè ogni intorno di un insieme compatto A contiene un intorno compatto di A che appartiene a $\mathcal{B}$.*

Una misura μ può fallire nell'essere regolare, ma si può definire la sua regolarizzazione come

$$\mu'(A) := \inf\{\mu(B) \,|\, \mathring{B} \supset A,\, B \in \mathcal{C}\}$$

per ogni insieme compatto A e si può altresì mostrare che essa è a tutti gli effetti una misura regolare. Così una premisura ν si dirà regolare se la sua regolarizzazione ν' definita come

$$\nu'(A) := \inf\{\nu(B) \,|\, \mathring{B} \supset A,\, B \in \mathcal{B}\}$$

per qualsiasi compatto A coincide con ν su $\mathcal{B}$. Anche in questo caso, la regolarizzazione di qualsiasi premisura è una misura regolare e se una misura regolare μ è un'estensione di una premisura ν, allora $\mu = \nu'$. A riguardo delle nozioni introdotte si può osservare che

(1) se ν è una premisura regolare, allora la sua regolarizzazione è l'unica misura regolare che estende ν;

(2) ogni misura regolare è una funzione esatta[5];

(3) una misura μ su $\mathcal{C}$ è regolare se e solo se è esatta e ciò avviene se e solo se μ è continua per successioni crescenti (in tal caso essa sarà anche detta *ipercontinua*).

Se ora X è un G-spazio (a sinistra), cioè uno spazio di Hausdorff localmente compatto su cui agisce a sinistra il gruppo G, e si assume che l'azione di gruppo sia transitiva[6] e semirigida[7], allora si ha il seguente risultato, ricordando che una misura μ su X si dice G-invariante (a sinistra) se e solo se $\mu(gA) = \mu(A)$ per ogni $g \in G$ e per ogni $A \subset X$ compatto.

[5] Una *funzione esatta* è una funzione $\mu : \mathcal{A} \to \mathbb{R}_+$, ove $\mathcal{A}$ è un reticolo, tale che $\emptyset \in \mathcal{A}$, $\mu(\emptyset) = 0$ e $\mu(A) = \mu(B) + \sup\{\mu(C) \,|\, C \in \mathcal{A},\, C \subset A \setminus B\}$ per ogni $A, B \in \mathcal{A}$ tali che $B \subset A$. Si ricordi che un *reticolo* è un insieme parzialmente ordinato $(X, \leq)$ tale che ogni coppia di elementi di X abbia estremo superiore e inferiore rispetto a $\leq$. In particolare un reticolo di insiemi è una famiglia non vuota $\mathcal{A}$ chiusa per unione e intersezione finite, dove la relazione d'ordine parziale è data dall'inclusione.

[6] Per ogni $x, y \in X$ esiste $g \in G$ tale che $gx = y$.

[7] Se A e B sono sottoinsiemi compatti e disgiunti di X e $x \in X$, allora esiste un intorno V di x tale che, per ogni $g \in G$, nessun insieme della forma gV interseca sia A che B.

Teorema 3.3.1. *Se l'azione di G su X è transitiva e semirigida, allora vi è una misura regolare su X che è G-invariante e non identicamente nulla.*

Tutto questo si contestualizza nel caso dei gruppi topologici qualora X sia un gruppo topologico G e su di esso venga fatto agire G stesso. In tal caso, osservando (2.3.1) e (2.3.2), il modo in cui G agisce su sè stesso è esattamente una traslazione a sinistra, che si è già mostrato essere transitiva,[8] e si può provare che se G è di Hausdorff e localmente compatto, allora l'azione data dalla traslazione a sinistra è semirigida. Di conseguenza vi è una misura regolare μ su G non identicamente nulla e che è invariante a sinistra, cioè

$$\mu(A) = \mu(gA),\ \forall A \in \mathcal{C}, \forall g \in G$$

Passando invece alla terminologia legata agli integrali, dopo aver verificato sommariamente l'esistenza di una misura di Haar invariante a sinistra per gruppi topologici localmente compatti, se $\mathcal{A}$ è una famiglia di sottoinsiemi di X, una funzione f a valori reali è $\mathcal{A}$-semplice se e solo se è combinazione lineare finita di funzioni caratteristiche di elementi di $\mathcal{A}$. Così $L(\mathcal{A})$ indicherà lo spazio vettoriale delle funzioni $\mathcal{A}$-semplici e se $\mathcal{A}$ è un reticolo di insiemi, allora $L(\mathcal{A}) = L(\mathcal{R})$, ove $\mathcal{R}$ è l'anello generato da $\mathcal{A}$ [9]. Ma $L(\mathcal{A})$ è anche un reticolo vettoriale, anzi un reticolo vettoriale con troncamento[10].

Definizione 3.3.3. *Un* preintegrale *(o preintegrale di Daniell-Stone) è un funzionale lineare positivo I* [11] *su un reticolo vettoriale di funzioni con troncamento tale che se $\{f_n\}_{n\in\mathbb{N}}$ è una successione di funzioni decrescente che converge puntualmente alla funzione nulla, allora*

$$\lim_{n\to\infty} I(f_n) = 0$$

Definizione 3.3.4. *Un* integrale *è un funzionale lineare positivo I su un reticolo vettoriale L di funzioni con troncamento (quindi è in particolare un preintegrale) con la proprietà di Beppo Levi, ovvero se $\{f_n\}_{n\in\mathbb{N}} \subset L$ è una successione non decrescente tale che $f(x) = \sup_{n\in\mathbb{N}} f_n(x) < \infty$ per ogni x, allora $f \in L$ e $I(f) = \lim_{n\to\infty} I(f_n)$.*

3.3.1 Dalla misura all'integrale

Se si possiede una misura μ su $\mathcal{A}$ modulare[12], allora vi è un unico funzionale lineare I_μ su $L(\mathcal{A})$ tale che $I_\mu(\chi_A) = \mu(A)$. Così, se ν è una premisura su $\mathcal{A}$, allora I_μ è un preintegrale su $L(\mathcal{A})$, ove μ è un'estensione di ν. Il passo successivo è dato dall'estendere un preintegrale I su L a un integrale I^1 su L^1,

[8] Ciò è stato fatto per dimostrare l'omogeneità di ogni gruppo topologico.

[9] Esso è il più piccolo anello che contiene $\mathcal{A}$; le operazioni di anello sono in questo caso unione e differenza insiemistica.

[10] Se $f \in L(\mathcal{A})$, allora anche $1 \wedge f \in L(\mathcal{A})$, ove $(1 \wedge f)(x) := \min\{1, f(x)\}$.

[11] Se $f \in L(\mathcal{A})$ e $f \geq 0$, allora $I(f) \geq 0$.

[12] Affinché $\mu : \mathcal{A} \to \mathbb{R}_+$ sia modulare, $\mathcal{A}$ deve essere un reticolo di insiemi con $\emptyset \in \mathcal{A}$, $\mu(\emptyset) = 0$ e $\mu(A) + \mu(B) = \mu(A \cup B) + \mu(A \cap B)$.

noto come *estensione di Daniell*. A tal fine, una funzione f appartiene a L^1 (e si dice anche che è I^1-integrabile) se e solo se esiste una successione $\{f_n\}_{n\in\mathbb{N}} \subset L$ di funzioni a norme sommabili tali che $f(x) = \sum_{n=0}^{\infty} f_n(x)$ per I-quasi ogni x. Per concludere non resta che sfruttare il seguente teorema.

Teorema 3.3.2. *L'estensione di Daniell di un preintegrale è un integrale.*

Questo basta per mostrare che, data una misura, da essa si è in grado di ricavare un integrale. Per provare invece che da una misura di Haar si può ottenere un integrale di Haar si richiedono dimostrazioni specifiche, atte a controllare la preservazione delle proprietà caratteristiche. Ma ciò esula dagli intenti attuali.

3.3.2 Dall'integrale alla misura

Sia I un integrale sul reticolo vettoriale di funzioni con troncamento L e sia $\mathcal{B} := \{B \mid \chi_B \in L\}$; un modo intuitivo per assegnare una misura agli insiemi di $\mathcal{B}$ è dato dal porre $\eta(B) := I(\chi_B)$. Ebbene, omettendo i passaggi per i quali si rimanda al Capitolo 4 di [10], la famiglia $\mathcal{B}$ è un δ-anello e η, anche detta *misura indotta* dall'integrale I, è una misura standard su $\mathcal{B}$, nel senso che se $\{A_n\}_{n\in\mathbb{N}}$ è una successione di insiemi disgiunti in $\mathcal{B}$ tale che $\sum_{n=0}^{\infty} \eta(A_n) < \infty$, allora $\bigcup_{n=0}^{\infty} A_n \in \mathcal{B}$. Anche in questo caso si richiederebbe la verifica per η delle proprietà caratterizzanti una misura di Haar, qualora I sia un integrale di Haar, ma ciò non sarà fatto.

Si può invece osservare come il procedimento delineato sia un modo per costruire misure. Infatti, in accordo con quanto asserito nella sezione precedente, una premisura μ sul reticolo $\mathcal{A}$ induce un preintegrale su $L(\mathcal{A})$, la cui estensione di Daniell è un integrale I. Ma a questo punto si ha che I induce una misura standard η, la quale è quindi un'estensione di μ.

Capitolo 4

Rappresentazioni lineari di gruppi compatti

My work always tried to unite the truth with the beautiful,
but when I had to choose one or the other,
I usually chose the beautiful.
Hermann K. H. Weyl

Per questo capitolo si è fatto riferimento a [9] per quanto riguarda la prima e la terza sezione. Per quanto riguarda la seconda invece si è tratto spunto da [7].

Come anticipato nel precedente capitolo, si è ora devoti alla dimostrazione dell'esistenza di appropriate rappresentazioni lineari per gruppi compatti. Avendo sempre in mente la Definizione 3.0.1, che sarà ovviamente cruciale, si approfondiranno alcuni aspetti dell'integrale di Haar e appoggiandosi sui fatti enunciati a riguardo dei gruppi topologici nel Capitolo 2 e presentando una cornice sui gruppi di matrici, si arriverà a provare il Teorema 4.3 di [9], vera porta verso il passo conclusivo, cioè la dimostrazione del fatto che

> *Un gruppo compatto verifica la no small subgroups property se e solo se è isomorfo a un sottogruppo chiuso di un gruppo lineare generale.*

Si proceda perciò nell'ordine descritto.

4.1 Aspetti ulteriori dell'integrale di Haar

Come accennato precedentemente, saranno ora enunciati e provati alcuni risultati che saranno poi indispensabili per quanto affrontato nella Sezione 4.3. Infatti, sarà innanzitutto necessario assicurarsi che l'ordine di integrazione sia veramente irrilevante (il risultato sarà provato solo per $n = 2$ e dunque per il solo prodotto di due gruppi topologici), così da giustificare numerose osservazioni future, e alla prova di questo fatto è votata la presente sezione.

Proposizione 4.1.1. *Siano A uno spazio topologico e G un gruppo compatto; sia inoltre $f : G \times A \to \mathbb{R}$ una funzione continua. Allora l'applicazione $F : A \to \mathbb{R}$ definita nel modo seguente*

$$F(a) := \int f(x,a)dx$$

è pure continua.

Dimostrazione. La dimostrazione è standard e a senso unico, non particolarmente profonda. Si fissi $a \in A$ e sia $\varepsilon > 0$ pure fissato. Allora per continuità di f e per compattezza di G esiste un intorno aperto $U \subset A$ di a tale che

$$|f(x,b) - f(x,a)| < \varepsilon, \qquad \forall b \in U,\, \forall x \in G$$

Di conseguenza è sufficiente osservare che

$$\begin{aligned} |F(b) - F(a)| &= \left| \int f(x,b)dx - \int f(x,a)dx \right| = \left| \int (f(x,b) - f(x,a))dx \right| \leq \\ &\leq \int |f(x,b) - f(x,a)|dx < \varepsilon \end{aligned}$$

perché si ricordi che l'integrale è normalizzato. □

Se A fosse in più compatto, allora F risulterebbe essere uniformemente continua. Se invece $A = \mathbb{R}^n$ e si suppone che $f(x, t_1, ..., t_n)$ sia di classe C^k (rispettivamente liscia) nelle ultime n variabili con derivate continue su $G \times \mathbb{R}^n$ fino all'ordine k, allora anche $F(t_1, ..., t_n) = \int f(x, t_1, ..., t_n)dx$ risulterebbe C^k (rispettivamente liscia). Al di là di quest'ultima osservazione, si può ora provare il seguente risultato.

Teorema 4.1.1. *Siano G e H gruppi topologici compatti e sia P il loro prodotto diretto. Sia altresì $f : P \to \mathbb{R}$ una funzione continua. Allora, poste $F(y) := \int f(x,y)dx$ e $F'(x) := \int f(x,y)dy$*

$$\int F(y)dy = \int \left(\int f(x,y)dx \right) dy = \iint f(x,y)dxdy = \int f(z)dz \tag{4.1.1}$$

$$\int F'(x)dx = \int \left(\int f(x,y)dy \right) dx = \iint f(x,y)dxdy = \int f(z)dz \tag{4.1.2}$$

Dimostrazione. Prima di procedere a tutti gli effetti con la dimostrazione si osservi che gli integrali di F e F' esistono, in quanto per la proposizione precedente tali funzioni sono continue. In secondo luogo $z = (x,y) \in P$ e quindi $\int f(z)dx$, che indicherebbe astrattamente l'integrale di f su P, risulta definito operativamente dalle relazioni suddette.

Per provare l'enunciato basterà verificare (4.1.1), in quanto per (4.1.2) si procede esattamente nella stessa direzione. Sia perciò

$$\int^* f(z)dz := \int \left(\int f(x,y)dx \right) dy$$

Se si prova che $\int^* f(z)dz$ soddisfa le proprietà sufficienti della Definizione 3.2.1, che per il Teorema 3.2.1 risultano essere dalla 1. alla 4. e in più la 6., allora si ha immediatamente la conclusione, grazie all'unicità dell'integrale. Ma la verifica di queste richieste è molto facile e ne saranno fornite solo un paio come esempio.

1. Sia $\alpha \in \mathbb{R}$, allora

$$\begin{aligned}\int^* \alpha f(z)dz &= \int\bigg(\int \alpha f(x,y)dx\bigg)dy = \int \alpha\bigg(\int f(x,y)dx\bigg)dy = \\ &= \alpha\int\bigg(\int f(x,y)dx\bigg)dy = \alpha\int^* f(z)dz\end{aligned}$$

6. Sia $c \in P$ con $c = (a,b)$ e $a \in G$, $b \in H$; per provare che $\int^* f(zc)dz = \int^* f(z)dz$ si può osservare che

$$\begin{aligned}\int^* f(zc)dz &= \int\bigg(\int f(xa,yb)dx\bigg)dy = \int\bigg(f(x,yb)dx\bigg)dy = \\ &= \int\bigg(\int f(x,y)dx\bigg)dy = \int^* f(z)dz\end{aligned}$$

In tutti questi passaggi immediati si è semplicemente utilizzato più volte il fatto che le medesime proprietà valgono per l'integrale di $f(x,y)$ rispetto a x e anche per l'integrale di $F(y) = \int f(x,y)dx$. Quindi per le dimostrazioni omesse non serve altro che applicare la medesima strategia. $\square$

Questo risultato sarà ampiamente utilizzato nel caso particolare in cui $G = H$ e quindi f risulterà essere una funzione di due variabili definita su G. La sezione sarà conclusa con la seguente osservazione.

Osservazione 4.1.1. L'integrale visto finora interessa funzioni $f : G \to \mathbb{R}$, ma può essere esteso intuitivamente a funzioni vettoriali $f : G \to \mathbb{R}^n$, semplicemente applicando il precedente integrale alle componenti. In questo modo, se $T : \mathbb{R}^n \to \mathbb{R}^m$ è un'applicazione lineare, allora per linearità dell'integrale si ha che

$$\int T(f(g))dg = T\bigg(\int f(g)dg\bigg)$$

Infatti l'i-esima componente di $T(f(g))$ è data dal prodotto della i-esima riga della matrice rappresentativa di T per $f(g)$, dunque da una combinazione lineare di funzioni a valori reali, alla quale si può applicare, come già detto, la linearità dell'integrale di Haar.

4.2 Gruppi di matrici ed esponenziale

I gruppi classici di matrici, quali quello lineare generale od ortogonale o speciale, sono noti e ad essi si è già accennato nel Capitolo 2, ma la loro trattazione deve essere ora approfondita.

Definizione 4.2.1. *Sia* $\mathbb{K}$ *un campo. Un'*algebra associativa $\mathcal{A}$ *su* $\mathbb{K}$ *è uno spazio vettoriale su* $\mathbb{K}$ *che è anche un anello, in modo tale che*

$$\forall x, y \in \mathcal{A},\, \forall \lambda \in \mathbb{K},\ \lambda(xy) = (\lambda x)y = x(\lambda y)$$

Equivalentemente si può dire che $\mathcal{A}$ *è un'algebra associativa su* $\mathbb{K}$ *se è uno spazio vettoriale su* $\mathbb{K}$ *dotato di una forma bilineare.*

Definizione 4.2.2. *Un'*algebra di Banach *su* $\mathbb{K}$ *è un'algebra associativa con unità* $\mathcal{A}$ *che è un anello unitario ed è equipaggiata con una norma, che rende il sottostante spazio vettoriale uno spazio di Banach*[1] *e soddisfa la disuguaglianza* $\|xy\| \leq \|x\|\|y\|$ *per ogni* $x, y \in \mathcal{A}$.

Un elemento $x \in \mathcal{A}$ è un'unità se è invertibile e l'insieme di tutte le unità di un'algebra $\mathcal{A}$, denotato con $\mathcal{A}^*$, è il più grande sottogruppo del semigruppo moltiplicativo di $\mathcal{A}$ contenente 1, ovvero l'unità rispetto alla moltiplicazione. Per una trattazione generale, è basilare la seguente proposizione, per la cui dimostrazione si rimanda a [7].

Proposizione 4.2.1. *Sia* $\mathcal{A}$ *un'algebra di Banach. Allora il gruppo delle unità* $\mathcal{A}^*$ *è un gruppo topologico ed è aperto in* $\mathcal{A}$.

Alla luce di questo fatto, la dimostrazione data nel Capitolo 2 del fatto che $GL(n, \mathbb{R})$ fosse un gruppo topologico appare quanto mai triviale. Ma la definizione di questo speciale gruppo di matrici (e degli altri ad esso associati) può essere affrontata con maggiore generalità. Infatti, se V è uno spazio di Banach su $\mathbb{K}$, allora $\mathrm{Hom}(V, V)$ è un'algebra di Banach rispetto alla norma $\|T\| := \sup_{\|x\| \leq 1} \|Tx\|$ e il suo gruppo delle unità, costituito da tutti gli operatori lineari continui invertibili, è detto *gruppo lineare generale* su V e denotato con $GL(V)$.

Nel caso in cui $V = \mathbb{K}^n$ (nei casi che saranno interessanti si avrà $\mathbb{K} = \mathbb{R}$ o $\mathbb{K} = \mathbb{C}$), allora $GL(V)$ è anche indicato con $GL(n, \mathbb{K})$ ed è detto *gruppo lineare generale di ordine n*, che può essere identificato canonicamente con il gruppo delle matrici non singolari $n \times n$ a coefficienti in $\mathbb{K}$. È in questa situazione che si può specificare il contesto generale fin qui delineato.

(1) *gruppo lineare speciale di ordine n su* $\mathbb{K}$:

$$SL(n, \mathbb{K}) := \{g \in GL(n, \mathbb{K}) \mid \det g = 1\}$$

(2) sia H uno spazio di Hilbert[2] su $\mathbb{K}$ con prodotto scalare $\langle \cdot, \cdot \rangle$, allora l'insieme di tutti gli elementi $g \in GL(H)$ tali che $\langle gx, gx \rangle = \langle x, x \rangle$ per ogni $x \in H$ è denotato con $U(H)$ ed è un sottogruppo di $GL(H)$, detto *gruppo unitario*.

[1] Uno *spazio di Banach* è uno spazio normato completo, in cui cioè ogni successione di Cauchy è convergente. Si ricordi che ogni spazio normato di dimensione finita è completo e quindi di Banach.

[2] Uno spazio H con prodotto scalare è detto essere uno *spazio di Hilbert* se è completo. Poiché ogni prodotto scalare induce una norma, allora ogni spazio di Hilbert è anche di Banach, mentre in generale non vale il viceversa.

1. se $H = \mathbb{R}^n$ con il prodotto scalare standard, allora $U(H)$ è denotato con $O(n)$ ed è detto il *gruppo ortogonale di ordine* n; in più si definisce il *gruppo ortogonale speciale di ordine* n come
$$SO(n) := O(n) \cap SL(n, \mathbb{R})$$
2. se $H = \mathbb{C}^n$ con il prodotto scalare hermitiano, allora $U(H)$ è denotato con $U(n)$ ed è detto il *gruppo unitario di ordine* n; in più si definisce il *gruppo unitario speciale di ordine* n come
$$SU(n) := U(n) \cap SL(n, \mathbb{C})$$

Tutti i sottogruppi di $GL(n, \mathbb{K})$ qui presentati sono compatti.

A riguardo dei gruppi di matrici è di fondamentale importanza l'esponenziale di matrici, introdotto per la prima volta da Giuseppe Peano. Si può infatti osservare che se $A \in \mathcal{M}(n \times n, \mathbb{K})$ è una matrice tale che i suoi coefficienti sono maggiorati in valore assoluto da c, allora, per semplice induzione, gli ingressi di A^k sono maggiorati da $(nc)^k$. Questo significa che i coefficienti di
$$\sum_{k=0}^{\infty} \frac{A^k}{k!} \tag{4.2.1}$$
sono maggiorati in valore assoluto dalla serie convergente e^{nc} e pertanto anche la serie (4.2.1) converge a una matrice, che sarà indicata con e^A per ovvia analogia.[3] In particolare la convergenza è uniforme su ogni sottoinsieme compatto di $\mathcal{M}(n \times n, \mathbb{R})$. Di conseguenza gli ingressi di e^A sono funzioni analitiche nei coefficienti di A e ciò permette di affermare che anche
$$\begin{cases} \exp : \mathcal{M}(n \times n, \mathbb{R}) \to \mathcal{M}(n \times n, \mathbb{R}) \\ A \mapsto \exp(A) = e^A \end{cases}$$
è analitica; inoltre, fatto banale, $e^0 = I$. A questo punto si possono però provare anche due risultati meno immediati, di cui il primo si offre ad applicazioni successive.

Proposizione 4.2.2. $\exp : \mathcal{M}(n \times n, \mathbb{K}) \to GL(n, \mathbb{K})$ *(ove $\mathbb{K} = \mathbb{R}$ o $\mathbb{K} = \mathbb{C}$), cioè l'esponenziale di matrici è a valori nel gruppo lineare generale di dimensione n; ciò significa che e^A è invertibile, qualunque sia A.*

Dimostrazione. Siano $A \in \mathcal{M}(n \times n, \mathbb{K})$ e $B \in GL(n, \mathbb{K})$, allora si può innanzitutto osservare che
$$\begin{aligned} e^{BAB^{-1}} &= \sum_{n=0}^{\infty} \frac{(BAB^{-1})^n}{n!} = \sum_{n=0}^{\infty} \frac{BA^nB^{-1}}{n!} \overset{*}{=} B\left(\sum_{n=0}^{\infty} \frac{A^n}{n!}\right)B^{-1} = \\ &= Be^AB^{-1} \end{aligned}$$

[3] Lo stesso risultato può essere dimostrato senza richiedere la maggiorazione degli ingressi di A; in tal caso si dovrebbe introdurre una norma matriciale, equivalente da un punto di vista topologico a una norma su $\mathbb{R}^{n^2}$, e sfruttando la disuguaglianza di Cauchy-Schwarz mostrare che la successione data dalle somme parziali di $\sum_{n=0}^{\infty} \frac{A^n}{n!}$ è di Cauchy. Per la completezza di $\mathcal{M}(n \times n, \mathbb{R}) \cong \mathbb{R}^{n^2}$ si conclude.

ove il passaggio $(*)$ è giustificato dal fatto che la serie è convergente. Se $A \in \mathcal{M}(n \times n, \mathbb{C})$, allora esiste $B \in GL(n, \mathbb{C})$ tale che BAB^{-1} sia triangolare superiore con autovalori $\lambda_1, ..., \lambda_n$ sulla diagonale (esattamente tutti gli autovalori, ripetuti se con molteplicità algebrica maggiore di 1) e da ciò segue che

$$Be^A B^{-1} = e^{BAB^{-1}} = \begin{pmatrix} e^{\lambda_1} & p_{12} & p_{13} & \dots & p_{1n} \\ 0 & e^{\lambda_2} & p_{23} & \dots & p_{2n} \\ 0 & 0 & e^{\lambda_3} & \dots & p_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & e^{\lambda_n} \end{pmatrix}$$

Quindi $e^{\lambda_1}, ..., e^{\lambda_n}$ sono gli autovalori di e^A e in particolare vale la seguente relazione

$$\det e^A = e^{Tr(A)}$$

ove $Tr(A) = \sum_{i=0}^n \lambda_i$. Poiché l'esponenziale su $\mathbb{C}$ è sempre non nullo, allora e^A è invertibile. Nel caso in cui $\mathbb{K} = \mathbb{R}$ invece, si sfrutta il fatto che ogni matrice può essere ridotta in forma canonica di Jordan. $\square$

Proposizione 4.2.3. *Se $A, B \in \mathcal{M}(n \times n, \mathbb{R})$ commutano, allora $e^{A+B} = e^A e^B$.*

Dimostrazione. Si premetta innanzitutto il seguente fatto, che si può provare per induzione: siano $A, B \in \mathcal{M}(n \times n, \mathbb{R})$ e sia $c \in \mathbb{R}_{++}$ tali che $|A_{ij}| \leq c, |B_{ij}| \leq c, \forall i, j \in \{1, ..., n\}$, allora per ogni $i, j \in \{1, ..., n\}$ e per ogni $m, s, k \in \mathbb{N}$ valgono le disuguaglianze

$$|(A^n)_{ij}| \leq (cn)^m, \ |(B^n)_{ij}| \leq (cn)^m, \ |(A^s B^k)_{ij}| \leq (cn)^{s+k} \tag{4.2.2}$$

Per ogni $n \in \mathbb{N}$ si definisca

$$\Omega_n := \sum_{s=0}^{2n} \frac{(A+B)^s}{s!} - \left(\sum_{s=0}^{n} \frac{A^s}{s!} \right) \left(\sum_{k=0}^{n} \frac{B^k}{k!} \right)$$

e si osservi che per la formula del binomio di Newton e per l'ipotesi di commutatività

$$\Omega_n = \sum_{k=0}^{n} \sum_{s=n+1}^{2n} \left(\frac{A^s}{s!} \frac{B^k}{k!} \right) + \sum_{s=0}^{n} \sum_{k=n+1}^{2n} \left(\frac{A^s}{s!} \frac{B^k}{k!} \right)$$

In secondo luogo $\lim_{n \to \infty} \Omega_n = e^{A+B} - e^A e^B$ e in virtù di (4.2.2) si ha la stima seguente

$$\begin{aligned} |(\Omega_n)_{ij}| &\leq \sum_{k=0}^{n} \sum_{s=n+1}^{2n} \left(\frac{(cn)^s}{s!} \frac{(cn)^k}{k!} \right) + \sum_{s=0}^{n} \sum_{k=n+1}^{2n} \left(\frac{(cn)^s}{s!} \frac{(cn)^k}{k!} \right) = \\ &= \sum_{s=0}^{2n} \frac{(2cn)^s}{s!} - \left(\sum_{s=0}^{n} \frac{(cn)^s}{s!} \right) \left(\sum_{k=0}^{n} \frac{(cn)^k}{k!} \right) \end{aligned}$$

Questo permette di concludere, perché

$$\lim_{n\to\infty} (\Omega_n)_{ij} = e^{2cn} - e^{cn}e^{cn} = 0, \quad \forall i, j \in \{1, ..., n\}$$

e quindi $(e^{A+B})_{ij} = (e^A e^B)_{ij}$, da cui la tesi. $\square$

4.3 Il teorema di rappresentazione

Allo scopo di provare il teorema chiave di questo paragrafo, che assicura l'esistenza di opportune rappresentazioni lineari di un gruppo compatto G nel gruppo lineare generale (un ambiente dove è certamente più facile operare), si devono innanzitutto definire le funzioni caratteristiche sui gruppi compatti. A tal fine, sia come sempre G un gruppo compatto e, dato $n \in \mathbb{N}$ (anche se nella maggior parte dei casi si avrà $n = 1$), si indichi con V lo spazio vettoriale reale infinitodimensionale delle funzioni continue $f : G \to \mathbb{R}^n$. Per $f, g \in V$ si può definire il seguente prodotto scalare

$$\langle f\, ,\, g\rangle := \int \langle f(x)\, ,\, g(x)\rangle dx$$

dove quello presente nella funzione integranda è l'usuale prodotto scalare di $\mathbb{R}^n$. In particolare si può anche definire $\|f\| := \sqrt{\langle f, f\rangle}$.

Definizione 4.3.1. *Sia $k : G\times G \to \mathbb{R}$ una funzione continua tale che $k(x, y) = k(y, x)$ per ogni $x, y \in G$. Tale applicazione è detta* funzione nucleo.

Per una certa funzione nucleo assegnata k si può allora definire il seguente operatore lineare $\mathscr{K} : V \to V$

$$(\mathscr{K} f)(x) := \int k(x, y)f(y)dy \tag{4.3.1}$$

che mappa la palla unitaria chiusa $\{f \,|\, \langle f, f\rangle \leq 1\}$ in un insieme di funzioni equilimitate (in un senso che sarà chiarito tra breve) ed equicontinue ed è simmetrico, in quanto $\langle \mathscr{K} f, g\rangle = \langle f, \mathscr{K} g\rangle$ per semplice scambio nell'ordine di integrazione, giustificato dal Teorema 4.1.1. La definizione di questo operatore è legittimata dall'esistenza dell'integrale di Haar, provata precedentemente; la definizione di $\mathscr{K}$ può però essere arricchita nel modo seguente.

Definizione 4.3.2. *Sia $\varphi \in V$ una funzione continua non identicamente nulla; essa è detta essere una* funzione caratteristica *di $\mathscr{K}$ relativa al valore caratteristico $\lambda \in \mathbb{R}$ se $\mathscr{K}\varphi = \lambda\varphi$.*

È palese come la definizione di funzione caratteristica sia analoga a quella di autovettore per un normale operatore lineare tra spazi vettoriali, così come quella di valore caratteristico è equivalente a quella di autovalore, come noto dall'Algebra Lineare. E infatti il teorema spettrale continua a valere anche nel caso infinitodimensionale. A riguardo di questi nuovi enti saranno elencate tre proprietà molto importanti, che saranno sfruttate nel seguito e che sono risultati abbastanza significativi di Analisi Funzionale. Sia allora $\mathscr{K}$ definito come sopra:

(a) per ogni $\varepsilon > 0$, i valori caratteristici λ di $\mathscr{K}$ tali che $|\lambda| \geq \varepsilon$ sono finiti;

(b) per ogni valore caratteristico $\lambda \neq 0$, le funzioni caratteristiche ad esso associate formano uno spazio vettoriale di dimensione finita;

(c) per i risultati precedenti, si può individuare una successione di valori caratteristici λ_i tali che $|\lambda_i| \to 0$ per $i \to \infty$ [4] e ad ognuno di questi si può associare un numero finito di funzioni caratteristiche $\varphi_{i1}, ..., \varphi_{in_i}$ tali da formare una base ortonormale dello spazio vettoriale associato a λ_i. Ma in più tali funzioni formano anche una base ortonormale di V, perché appartenenti ad autospazi ortogonali. Di conseguenza, se $g = \mathscr{K} f$ per qualche $f \in V$, allora la serie di Fourier $\sum_{i=1}^{\infty} \sum_{j=1}^{n_i} \langle g, \varphi_{ij} \rangle \varphi_{ij}$ converge uniformemente a g.[5]

La dimostrazione di quanto affermato a riguardo dell'operatore $\mathscr{K}$ merita un proprio paragrafo.

4.3.1 L'operatore $\mathscr{K}$

Quanto si andrà ora a provare, può essere facilmente reperito in molti testi; si è però scelto lo Chevalley [11] per l'importanza storica e la chiarezza espositiva. In tale libro tutti i risultati seguenti e già precedentemente annunciati sono presentati come lemmi, finalizzati alla dimostrazione della seguente versione del teorema di Peter-Weyl, adattata al caso dei gruppi di Lie compatti.

Teorema 4.3.1 (Peter-Weyl)**.** *Siano G un gruppo di Lie compatto e f una funzione continua definita su di esso. Per ogni $\varepsilon > 0$, nell'anello rappresentativo di G [6] esiste una funzione g tale che $|f(x) - g(x)| \leq \varepsilon$ per ogni $x \in G$.*

Innanzitutto si provi un fatto basilare.

Proposizione 4.3.1. *L'operatore $\mathscr{K}$ è ben definito, ovvero per ogni funzione $f \in V$, $\mathscr{K} f \in V$. Inoltre mappa la palla unitaria $\{f \mid \langle f, f \rangle \leq 1\}$ in un insieme limitato di funzioni equicontinue.*

[4] Infatti, per il punto (a) è sufficiente individuare una successione decrescente di numeri reali $\{c_i\}_{i \in \mathbb{N}}$ tali che $c_i \to 0$. Così facendo si può iniziare da c_o e considerare i valori caratteristici maggiori in modulo di c_0; il passo successivo è dato dal prendere c_1 e i valori caratteristici maggiori in modulo di c_1: tra questi vi sono certamente i precedenti, in quanto $c_1 \leq c_0$, ma possono essercene altri compresi in modulo tra c_1 e c_0. Questi saranno aggiunti a quelli precedentemente individuati. Non resta che iterare il procedimento. Poiché lo spettro di valori caratteristici di $\mathscr{K}$ è infinito (si è su di uno spazio vettoriale infinito-dimensionale), allora si può essere certi che non può accadere $|\lambda_i| \to c > 0$, perché se così fosse si avrebbe una contraddizione con quanto detto al punto (a).

[5] Questo significa che la successione delle somme parziali $\sum_{i=1}^{k} \sum_{j=1}^{n_i} \langle g, \varphi_{ij} \rangle \varphi_{ij}$ converge uniformemente a g per $k \to \infty$.

[6] Esso è l'anello sul campo complesso generato dai coefficienti di tutte le rappresentazioni di G, ovvero è l'anello i cui elementi sono le funzioni a valori complessi definite su G, che possono essere espresse come polinomi nei coefficienti delle rappresentazioni del gruppo.

Dimostrazione. Innanzitutto si provi che $\mathscr{K} f$ è continua, poiché così $\mathscr{K} f \in V$. Sia allora $\varepsilon > 0$ e sia U_ε un intorno dell'unità in G tale che $|k(zx, y) - k(x, y)| < \varepsilon$ per ogni $z \in U_\varepsilon$ e per ogni $x, y \in G$. Se così non fosse, esisterebbe un certo $\varepsilon_0 > 0$ tale che per ogni intorno dell'unità U esistono $x, y \in G$, $z \in U$ tali che $|k(zx, y) - k(x, y)| \geq \varepsilon_0$. Questo consente di costruire le successioni $\{x_n\}_n, \{y_n\}_n, \{z_n\}_n$ con $z_n \to e$ tali che $|k(z_n x_n, y_n) - k(x_n, y_n)| \geq \varepsilon_0$ per ogni $n \in \mathbb{N}$. Ma poiché G è compatto, allora $\{x_n\}_n$ e $\{y_n\}_n$ ammettono sottosuccessioni $\{x_{n_k}\}_k$ e $\{y_{n_k}\}_k$ convergenti rispettivamente a x e y. Di conseguenza

$$\lim_{k \to \infty} |k(z_{n_k} x_{n_k}, y_{n_k}) - k(x_{n_k}, y_{n_k})| = |k(ex, y) - k(x, y)| \geq \varepsilon_0 > 0,$$

il che è però assurdo. Pertanto, se $z \in U_\varepsilon$, si ha la seguente disuguaglianza

$$\begin{aligned} |\mathscr{K} f(zx) - \mathscr{K} f(x)| &\leq \int |(k(zx, y) - k(x, y)) f(y)| dy \leq \varepsilon \int |f(y)| dy = \\ &= \varepsilon \langle 1, f \rangle \leq \varepsilon \|f\| \end{aligned} \tag{4.3.2}$$

ove l'ultimo passaggio è valido in virtù della disuguaglianza di Schwarz. Questo è sufficiente per concludere che $\mathscr{K} f$ è continua.

Per quanto riguarda invece il secondo asserto, sia $M := \max_{G \times G} |k|$, il quale esiste per continuità di k su di un compatto. Allora

$$|\mathscr{K} f(x)| \leq M \int |f(y)| dy \leq M \|f\| \tag{4.3.3}$$

e questo dimostra che la palla unitaria viene mappata da $\mathscr{K}$ in un insieme limitato da M. Inoltre, se in (4.3.2) si impone $\|f\| \leq 1$, allora si ottiene anche l'equicontinuità, come richiesto. $\square$

Si passi invece ora alla concreta dimostrazione delle proprietà (a), (b) e (c). A tal fine sia Φ l'insieme delle funzioni caratteristiche di $\mathscr{K}$ relative ad autovalori non nulli. Sia quindi $\Phi^* \subset \Phi$ un insieme massimale rispetto alla proprietà che le funzioni caratteristiche che vi appartengono siano ortonormali rispetto a $\langle \cdot, \cdot \rangle$: l'esistenza è assicurata dal lemma di Zorn. Allora (a) e (b) saranno provate in un colpo solo, ma articolando la dimostrazione in tre enunciati.

Lemma 4.3.1. *Sia $\mathcal{F} \subset V$ un insieme limitato di funzioni equicontinue e sia $\varepsilon > 0$. Se $\max_G |f - g| > \varepsilon$ per ogni coppia di funzioni distinte in un certo $\mathcal{F}_1 \subset \mathcal{F}$, allora $\mathcal{F}_1$ è finito.*

Dimostrazione. Sia M un valore che limita in modulo tutte le funzioni di $\mathcal{F}$. Se $x_0 \in G$, allora $\{f(x_0) \mid f \in \mathcal{F}\}$ è contenuto in $[-M, M] \subset \mathbb{R}$. Di conseguenza, per compattezza di $[-M, M]$, esiste un sottoinsieme finito $\mathcal{G}_0$ di $\mathcal{F}$ tale che per ogni $f \in \mathcal{F}$ esiste $f_1 \in \mathcal{G}_0$ tale che $|f(x_0) - f_1(x_0)| < \frac{\varepsilon}{6}$. Sia ora $x \in x_0 U_{\varepsilon/6}$, ove $U_{\varepsilon/6}$ è un intorno dell'unità tale che per ogni $x \in G$ e per ogni $f \in \mathcal{F}$, l'oscillazione di f su $x U_{\varepsilon/6}$ è minore di ε; esso esiste per ipotesi di equicontinuità. Allora

$$|f(x) - f_1(x)| \leq |f(x) - f(x_0)| + |f(x_0) - f_1(x_0)| + |f_1(x_0) - f_1(x)| < \frac{\varepsilon}{2}$$

D'altra parte a ogni coppia di funzioni $(f,g) \in \mathcal{F}_1 \times \mathcal{F}_1$ si può associare un punto $x = x_{(f,g)} \in G$ tale che $|f(x) - g(x)| \geq \varepsilon$. Visto che $\mathcal{G}_0$ contiene un numero finito di funzioni, sia n, allora non possono esserci più di n^2 coppie $(f,g) \in \mathcal{F}_1 \times \mathcal{F}_1$ tali che $x_{(f,g)} \in x_0 U_{\varepsilon/6}$, perché se così non fosse, esisterebbe una coppia (f_0, g_0) tale che $|f_0(x) - f_1(x)| < \frac{\varepsilon}{2}$, $|g_0(x) - f_1(x)| < \frac{\varepsilon}{2}$ per la stessa $f_1 \in \mathcal{G}_0$. Ma ciò significherebbe $|f_0(x) - g_0(x)| < \varepsilon$, il che è assurdo, dato che si deve avere $|f_0(x) - g_0(x)| \geq \varepsilon$.

In conclusione, poiché G può essere ricoperto da un numero finito di insiemi della forma $x_0 U_{\varepsilon/6}$, a ciascuno di questi si può associare solo un numero finito di coppie $(f,g) \in \mathcal{F}_1 \times \mathcal{F}_1$ e pur tuttavia ogni coppia di $\mathcal{F}_1 \times \mathcal{F}_1$ è associata ad almeno uno di questi insiemi, allora $\mathcal{F}_1$ è finito. □

Si forniscano poi due lemmi necessari alla dimostrazione del teorema conclusivo di questa sezione. Per comprendere questi, si osservi banalmente che $\|\mathscr{K} f\| \leq M\|f\|$ e quindi $\|\mathscr{K} f\|$ resta limitato quando f è tale che $\|f\| = 1$. Sia $\|k\| := \sup_{\{f : \|f\|=1\}} \|\mathscr{K} f\|$ e si osservi che $\|\mathscr{K} f\| \leq \|k\|\|f\|$.

Lemma 4.3.2. $\|k\| = \sup_{\{f:\|f\|=1\}} \langle \mathscr{K} f, f\rangle$, *cioè* $\|k\|$ *è il minore dei maggioranti dei valori assunti da* $\langle \mathscr{K} f, f\rangle$ *quando* $\|f\| = 1$.

Dimostrazione. Se $\|f\| = 1$, allora per la disuguaglianza di Schwarz e per l'osservazione precedente $|\langle \mathscr{K} f, f\rangle| \leq \|\mathscr{K} f\|\|f\| \leq \|k\|$. Dunque $\|k\|$ è un maggiorante di $|\langle \mathscr{K} f, f\rangle|$ per $\|f\| = 1$; per provare che esso è il minore di tali maggioranti, sia $c = \sup_{\{f:\|f\|=1\}} |\langle \mathscr{K} f, f\rangle| \leq \|k\|$. Allora, dato che $\|\mathscr{K} f\| \leq \|k\|\|f\|$, segue che $|\langle \mathscr{K} f, f\rangle| \leq c\|f\|^2$ per ogni $f \in V$. Siano ora f, g tali che $\|f\| = 1$ e $\|g\| = 1$, allora si possono ottenere facilmente le seguenti disuguaglianze.

$$\langle \mathscr{K}(f+g), f+g\rangle = \langle \mathscr{K} f, f\rangle + 2\langle \mathscr{K} f, g\rangle + \langle \mathscr{K} g, g\rangle \leq c\|f+g\|^2$$

$$\langle \mathscr{K}(f-g), f-g\rangle = \langle \mathscr{K} f, f\rangle + \langle \mathscr{K} g, g\rangle - 2\langle \mathscr{K} f, g\rangle \geq -c\|f-g\|^2$$

da cui

$$4\langle \mathscr{K} f, g\rangle \leq c(\|f+g\|^2 + \|f-g\|^2) = 2c(\|f\|^2 + \|g\|^2) = 4c$$

Se si assume che $\mathscr{K} f$ non sia identicamente nulla e si prende $g = \mathscr{K} f / \|\mathscr{K} f\|$, si ottiene $\|\mathscr{K} f\| \leq c$. D'altra parte, se $\mathscr{K} f \equiv 0$, la stessa disuguaglianza è banalmente verificata e quindi la tesi è ugualmente provata. □

Lemma 4.3.3. *Almeno uno tra* $\|k\|$ *e* $-\|k\|$ *è un autovalore di* k.

Dimostrazione. Per il lemma precedente si può individuare una successione $\{f_n\} \subset V$ tale che $\|f_n\| = 1$ per ogni n e $\langle \mathscr{K} f_n, f_n\rangle$ converge a $\|k\|$ oppure a $-\|k\|$. Sia $c := \lim_{n\to\infty} \langle \mathscr{K} f_n, f_n\rangle$. Poiché da una successione di funzioni equicontinue e limitate rispetto a $\|\cdot\|$ è possibile estrarre una sottosuccessione che converge uniformemente su G [7], allora a meno di sostituire $\{f_n\}$ con una sua sottosuccessione si può assumere senza perdita di generalità che $\{\mathscr{K} f_n\}$

[7]Si veda per esempio il Lemma 2 a pag. 205 di [11]

converga uniformemente su G a una funzione φ che ovviamente appartiene a V. Di conseguenza

$$\lim_{n\to\infty} \max_G |\varphi - \mathscr{K} f_n| = 0$$

Si osservi poi che $\langle f, g\rangle$ è continua rispetto alla metrica indotta dal massimo, poiché $\|f\|^2 = \int f^2(x)dx \leq (\max_G |f|)^2$ e questo permette di affermare che

$$|\langle f_1 - f_2, g_1 - g_2\rangle| \leq \|f_1 - f_2\|\|g_1 - g_2\| \leq \max_G |f_1 - f_2| \max_G |g_1 - g_2|$$

Dato che si stanno considerando funzioni a valori reali, allora

$$\|\mathscr{K} f_n - cf_n\|^2 = \|\mathscr{K} f_n\|^2 + c^2\|f_n\|^2 - 2c\langle \mathscr{K} f_n, f_n\rangle \tag{4.3.4}$$

e al limite per $n \to \infty$ il membro di destra tende a $\|\varphi\|^2 - c^2$. Ne segue che $\|\varphi\| \geq |c|$, da cui φ non è identicamente nulla se $c \neq 0$. D'altra parte $\|\mathscr{K} f_n\|^2 \leq \|k\|^2 \leq c^2$ per il lemma precedente e così (4.3.4) può alternativamente essere riscritta come

$$\|\mathscr{K} f_n - cf_n\|^2 \leq 2c^2 - 2c\langle \mathscr{K} f_n, f_n\rangle$$

ove ora il membro di destra tende a 0 con $1/n$. Se ne deduce che $\lim_{n\to\infty} \|\mathscr{K} f_n - cf_n\| = 0$ e quindi anche che $\lim_{n\to\infty} \|\mathscr{K}(\mathscr{K} f_n) - c\mathscr{K} f_n\| = 0$. E poiché $\lim_{n\to\infty} \|\mathscr{K} f_n - \varphi\| = 0$, allora $\lim_{n\to\infty} \max_G |\mathscr{K}(\mathscr{K} f_n) - \mathscr{K}\varphi| = 0$, da cui

$$\|\mathscr{K}\varphi - c\varphi\| = \lim_{n\to\infty} \|\mathscr{K}(\mathscr{K} f_n - c\mathscr{K} f_n\| = 0$$

Ciò prova che $\mathscr{K}\varphi = c\varphi$. La tesi è così provata se $c \neq 0$, ma in caso contrario si ha che $\|k\| = 0$ e $\mathscr{K} f \equiv 0$ per ogni f, da cui l'enunciato segue banalmente. $\square$

Proposizione 4.3.2. *Sia $\varepsilon > 0$. Allora in Φ^* vi è solo un numero finito di funzioni caratteristiche associate a valori caratteristici maggiori in modulo di ε.*

Dimostrazione. Siano $\{\varphi_i\}_{i\in\mathbb{N}} \subset \Phi^*$ tali che $\mathscr{K}\varphi_i = \lambda_i\varphi_i$ e $|\lambda_i| > \varepsilon$ per ogni $i \in \mathbb{N}$. Allora $\mathscr{K}(\varphi_i - \varphi_j) = \lambda_i\varphi_i - \lambda_j\varphi_j$, da cui $\|\mathscr{K}(\varphi_i - \varphi_j)\|^2 = \lambda_i^2 + \lambda_j^2 > 2\varepsilon^2$ su tutto G. Dunque $\max_G \|\mathscr{K}(\varphi_i - \varphi_j)\| > \sqrt{2}\varepsilon$ per ogni coppia di funzioni in Φ^* e poiché si è provato che $\mathscr{K}$ mappa la palla unitaria chiusa, in cui è contenuto Φ^*, in un insieme limitato di funzioni, allora per il Lemma 4.3.1 si ha la conclusione. $\square$

Proposizione 4.3.3. *Ogni funzione $f \in \Phi$ è combinazione lineare di un numero finito di funzioni appartenenti a Φ^*.*

Dimostrazione. Sia $f \in \Phi$ e sia λ il suo valore caratteristico. Per la proposizione precedente, a λ è associato solo un numero finito di funzioni caratteristiche, siano $\varphi_1, ..., \varphi_n$; si definisca quindi $f' := f - \sum_{i=1}^n \langle f, \varphi_i\rangle\varphi_i$. In primo luogo si può osservare che $\mathscr{K} f' = \lambda f'$, in quanto $\mathscr{K} f = \lambda f$ e $\mathscr{K}\varphi_i = \lambda\varphi_i$; in secondo luogo, f' è ortogonale a φ_i per ogni $i = 1, ..., n$, in quanto

$$\langle f', \varphi_i\rangle = \langle f, \varphi_i\rangle - \sum_{j=1}^n \langle f, \varphi_j\rangle\langle\varphi_j, \varphi_i\rangle = \langle f, \varphi_i\rangle - \sum_{j=1}^n \langle f, \varphi_j\rangle\delta_{i,j} = \langle f, \varphi_i\rangle - \langle f, \varphi_i\rangle = 0$$

Se poi $\psi \in \Phi^*$ è una qualsiasi funzione distinta da $\varphi_1, ..., \varphi_n$, allora il suo valore caratteristico sarà $\mu \neq \lambda$. Di conseguenza, si può constatare che

$$\langle f', \psi \rangle = \frac{1}{\mu} \langle f', \mathscr{K}\psi \rangle = \frac{1}{\mu} \langle \mathscr{K} f', \psi \rangle = \frac{\lambda}{\mu} \langle f', \psi \rangle$$

da cui si deduce che $\langle f', \psi \rangle = 0$, perché $\lambda \neq \mu$. Quindi f' è ortogonale a ogni funzione di Φ^* e se non si avesse $f' \equiv 0$, si potrebbe allora considerare $\Phi^* \cup \{f'/\|f'\|\}$: questa è un'estensione di Φ^* che soddisfa le stesse proprietà definenti quest'ultimo. Ma ciò violerebbe la massimalità di Φ^* e quindi si è autorizzati a concludere che $f' \equiv 0$; l'enunciato segue banalmente da questo fatto.

Prima di concludere si osservi che la dimostrazione fornisce anche i coefficienti della combinazione lineare: essi sono $\langle f, \varphi_i \rangle$ per $i = 1, ..., n$. □

Pertanto non resta che mostrare la correttezza di (c). Prima si osservi però che la Proposizione 4.3.2 permette di affermare che Φ è numerabile e quindi i suoi elementi possono essere ordinati in una successione $\{\varphi_n\}_n$ (che può anche essere finita); per ognuna di queste funzioni, il rispettivo valore caratteristico sarà indicato con λ_n.

Lemma 4.3.4 (disuguaglianza di Bessel)**.** *Sia $f \in V$. Allora $\sum_{i=1}^{|\Phi^*|} |\langle f, \varphi_i \rangle|^2$ è convergente; anzi, $\sum_{i=1}^{|\Phi^*|} |\langle f, \varphi_i \rangle|^2 \leq \|f\|^2$.*

Dimostrazione. Si costruisca la successione $\{g_n\}_{n \in \mathbb{N}}$, ponendo

$$g_n := f - \sum_{i=1}^{n} \langle f, \varphi_i \rangle \varphi_i$$

se Φ^* è infinito, altrimenti la successione è costituita da un numero finito di termini: tanti quante le funzioni in Φ^*. Poiché $\langle g_n, \varphi_i \rangle = 0$ per $i = 1, ..., n$ ed evidentemente $f = g_n + \sum_{i=1}^{n} \langle f, \varphi_i \rangle \varphi_i$, allora

$$\|f\|^2 = \|g_n\|^2 + \sum_{i=1}^{n} |\langle f, \varphi_i \rangle|^2$$

Passando al limite nel caso in cui Φ^* è infinito e altrimenti considerando $g_{|\Phi^*|}$, si ha la conclusione, perché al membro di destra si ha la serie dell'enunciato e l'uguaglianza fornisce la maggiorazione. □

Teorema 4.3.2. *Se $f \in V$, allora $\sum_{i=1}^{|\Phi^*|} \langle \mathscr{K} f, \varphi_i \rangle \varphi_i$ converge uniformemente su G a $\mathscr{K} f$.*

Dimostrazione. Innanzitutto

$$\begin{aligned}
\sum_{i=j}^{n} \langle \mathscr{K} f, \varphi_i \rangle \varphi_i &= \sum_{i=j}^{n} \langle \mathscr{K} f, \varphi_i \rangle \frac{\mathscr{K} \varphi_i}{\lambda_i} = \sum_{i=j}^{n} \langle f, \mathscr{K} \varphi_i \rangle \frac{\mathscr{K} \varphi_i}{\lambda_i} = \\
&= \sum_{i=j}^{n} \langle f, \varphi_i \rangle \mathscr{K} \varphi_i = \mathscr{K} \left(\sum_{i=j}^{n} \langle f, \varphi_i \rangle \varphi_i \right)
\end{aligned}$$

e quindi, in virtù di (4.3.3), definendo come nel contesto precedente $M := \max_{G\times G}|k|$, si ha che

$$\max_G\left|\sum_{i=j}^{n}\langle\mathscr{K}f,\varphi_i\rangle\varphi_i\right|\le M\left\|\sum_{i=j}^{n}\langle f,\varphi_i\rangle\varphi_i\right\|=M\left(\sum_{i=j}^{n}|\langle f,\varphi_i\rangle|^2\right)$$

Alla luce della disuguaglianza di Bessel, che prova come $\sum_{i=1}^{|\Phi^*|}|\langle f,\varphi_i\rangle|^2$ sia convergente, passando al limite per $j\to\infty$ (se Φ^* è infinito) nella disuguaglianza precedente, al membro di destra si ottiene il resto i-esimo della serie, che è infinitesimo. Quindi anche la serie $\sum_{i=1}^{|\Phi^*|}\langle\mathscr{K}f,\varphi_i\rangle\varphi_i$ è convergente uniformemente (ovviamente l'enunciato acquista spessore quando la serie è genuina e non una semplice somma finita). Non resta che provare che la funzione alla quale converge è $\mathscr{K}f$.

Sia

$$k_n(x,y):=k(x,y)-\sum_{i=1}^{n}\lambda_i\varphi_i(x)\varphi_i(y)$$

Evidentemente $k_n(x,y)=k_n(y,x)$ [8] e ad ogni funzione nucleo k_n si può associare un operatore $\mathscr{K}_n$ in modo del tutto naturale. Se si sceglie arbitrariamente $\varphi\in V$, allora $\mathscr{K}_n\varphi=\mathscr{K}\varphi-\sum_{i=1}^{n}\lambda_i\langle\varphi,\varphi_i\rangle\varphi_i$ e quindi

$$\langle\mathscr{K}_n\varphi,\varphi_i\rangle=\langle\mathscr{K}\varphi,\varphi_i\rangle-\lambda_i\langle\varphi,\varphi_i\rangle=\langle\varphi,\mathscr{K}\varphi_i\rangle-\lambda_i\langle\varphi,\varphi_i\rangle=0,\quad \text{per } i=1,...,n$$

perché sostanzialmente $\mathscr{K}_n$ proietta $\mathscr{K}\varphi$ sui vettori successivi all'n-esimo, annullando quindi le prime n coordinate. In particolare, se ψ è una funzione caratteristica di $\mathscr{K}_n$ associata a un valore caratteristico $\mu\neq 0$, allora $\langle\psi,\varphi_i\rangle=0$ per $i=1,...,n$ (in quanto $\varphi_1,...,\varphi_n$, come funzioni caratteristiche di $\mathcal{K}_n$, sono associate all'autovalore 0), $\mathscr{K}\psi=\mathscr{K}_n\psi=\mu\psi$ e ψ è una funzione caratteristica di $\mathscr{K}$ associata a μ. Ne segue, per la Proposizione 4.3.3, che ψ è combinazione lineare di un numero finito di funzioni $\varphi_{\mu_1},...,\varphi_{\mu_r}$ associate a μ, ovvero $\psi=\sum_{i=1}^{r}c_i\varphi_{\mu_i}$ con $c_i=\langle\psi,\varphi_{\mu_i}\rangle$ e quindi $c_i=0$ per $\mu_i\le n$ per quanto osservato poco sopra.

Sia $\varepsilon>0$ e si scelga n maggiore di tutti i pedici i per cui $|\lambda_i|\ge\varepsilon$ (di questi vi è infatti solo un numero finito), allora si può dedurre che $|\mu|<\varepsilon$, perché $\varphi_i,...,\varphi_n$, che hanno autovalori associati $\lambda_1,...,\lambda_n$ rispetto a $\mathscr{K}$, sono invece funzioni caratteristiche dell'autovalore nullo rispetto a $\mathscr{K}_n$, come già spiegato. Di conseguenza, per il Lemma 4.3.3 $\|k_n\|\le\varepsilon$ e quindi $\lim_{n\to\infty}\|\mathscr{K}_nf\|=0$, perché per $\varepsilon\to 0$ si ha che $n\to\infty$. Questo è però corretto se Φ^* è infinito; altrimenti se $|\Phi^*|=n$, allora $\mathscr{K}_nf=0$. Ma per quanto osservato poc'anzi,

$$\mathscr{K}_nf=\mathscr{K}f-\sum_{i=1}^{n}\lambda_i\langle f,\varphi_i\rangle\varphi_i=\mathscr{K}f-\sum_{i=1}^{n}\langle f,\mathscr{K}\varphi_i\rangle\varphi_i=\mathscr{K}f-\sum_{i=1}^{n}\langle\mathscr{K}f,\varphi_i\rangle\varphi_i$$

da cui

$$\lim_{n\to\infty}\|\mathscr{K}f-\sum_{i=1}^{n}\langle\mathscr{K}f,\varphi_i\rangle\varphi_i\|=0$$

[8] Questa simmetria sarebbe valida anche nel caso più generale in cui V fosse lo spazio vettoriale delle funzioni su G a valori complessi, purchè riscritta come $k_n(x,y)=\overline{k_n(y,x)}$ e a patto di definire $k_n(x,y):=k(x,y)-\sum_{i=1}^{n}\lambda_i\varphi_i(x)\overline{\varphi_i(y)}$.

che dimostra la tesi. $\square$

In questo modo si sono colmate le precedenti lacune dimostrative. Si riprenda il filo della trattazione.

Ricordando come sono state definite le traslazioni a sinistra e a destra, in analogia si possono definire le seguenti "traslazioni":

$$L_g : V \to V, \qquad L_g f(x) := f(g^{-1}x)$$

$$R_g : V \to V, \qquad R_g f(x) := f(xg)$$

Per queste è immediato osservare che valgono le relazioni (di omomorfismo)

$$L_g \circ L_h = L_{hg}, \qquad R_g \circ R_h = R_{hg}$$

e quindi $L_{(\cdot)}$ e $R_{(\cdot)}$ costituiscono due rappresentazioni lineari di G, in quanto ad ogni elemento $g \in G$ associano una trasformazione lineare dello spazio vettoriale infinito-dimensionale V. D'ora in poi si assumerà inoltre che la funzione nucleo abbia la forma $k(x, y) = h(xy^{-1})$, ove $h : G \to \mathbb{R}$ è tale che $h(x) = h(x^{-1})$: questo garantisce che k sia simmetrica. Ancora, se $A : \mathbb{R}^n \to \mathbb{R}^n$ è una qualsiasi applicazione lineare, allora $f \mapsto Af$ è una nuova trasformazione lineare da V in sè stesso che sarà ancora denotata con A. Con queste precisazioni si può allora dimostrare il seguente lemma.

Lemma 4.3.5. *Valgono i seguenti fatti:*

1. *$R_y \circ \mathscr{K} = \mathscr{K} \circ R_y$ per ogni $y \in G$ (R_y e $\mathscr{K}$ commutano);*
2. *$A \circ \mathscr{K} = \mathscr{K} \circ A$ per ogni trasformazione lineare $A : V \to V$ (A e $\mathscr{K}$ commutano);*
3. *se in più h è tale che $h(yxy^{-1}) = h(x)$ per ogni $x \in G$, allora vale anche $L_y \circ K = K \circ L_y$ (L_y e $\mathscr{K}$ commutano).*

Dimostrazione. Si inizi con il provare il primo punto, cioè che $\mathscr{K}(R_y f) = R_y(\mathscr{K} f)$ per ogni funzione $f \in V$, dunque che $(\mathscr{K}(R_y f))(x) = (R_y(\mathscr{K} f))(x)$ per ogni funzione $f \in V$ e per ogni $x \in G$.

$$\begin{aligned}(\mathscr{K}(R_y f))(x) &= \int h(xz^{-1})f(zy)dz = \int h(xy(zy)^{-1})f(zy)dz = \\ &= \int h((xy)z^{-1})f(z)dz = \mathscr{K} f(xy) = (R_y(\mathscr{K} f))(x)\end{aligned}$$

Alla terza uguaglianza si è semplicemente utilizzato l'invarianza per traslazioni dell'integrale di Haar (in questo caso traslazione a destra di y). Per il secondo punto si procede come di seguito, ricordando l'Osservazione 4.1.1:

$$\begin{aligned}(\mathscr{K}(Af))(x) &= \int h(xy^{-1})A(f(y))dy = \int A(h(xy^{-1})f(y))dy = \\ &= A \int h(xy^{-1})f(y)dy = (A(\mathscr{K} f))(x)\end{aligned}$$

Alla seconda uguaglianza si è sfruttata la linearità di A, mentre al passaggio successivo è intervenuta la suddetta osservazione. Per l'ultimo punto non resta che muoversi nella seguente direzione:

$$\begin{aligned}(\mathscr{K}(L_y f))(x) &= \int h(xz^{-1})f(y^{-1}z)dz = \int h(yy^{-1}x(y^{-1}z)^{-1}y^{-1})f(y^{-1}z)dz = \\ &= \int h(yy^{-1}xz^{-1}y^{-1})f(z)dz = \int h(y^{-1}xz^{-1})f(z)dz = \\ &= (\mathscr{K}f)(y^{-1}x) = (L_y(\mathscr{K}f))(x)\end{aligned}$$

La terza uguaglianza è giustificata dall'invarianza per traslazioni (a sinistra), mentre al passaggio successivo si è sfruttata l'ipotesi su h. La dimostrazione è quindi conclusa. $\square$

Lemma 4.3.6. *Valgono i seguenti fatti:*

(1) indicato con $V(\lambda)$ lo spazio vettoriale delle funzioni caratteristiche associate a λ, si può affermare che R_y e A mappano $V(\lambda)$ in sè stesso, ovvero $R_y, A : V(\lambda) \to V(\lambda)$;

(2) indicato con V_ε il sottospazio vettoriale di V, una cui base è data dalle funzioni caratteristiche corrispondenti ai valori caratteristici $|\lambda| \geq \varepsilon$, esso ha dimensione finita ed è ancora mappato in sè stesso da R_y e A;

(3) $V = V_\varepsilon \oplus V_\varepsilon^\perp$, ove $V_\varepsilon^\perp$ è il sottospazio ortogonale a V_ε in V;[9]

(4) R_y e A mappano $V_\varepsilon^\perp$ in sè stesso, ovvero $R_y, A : V_\varepsilon^\perp \to V_\varepsilon^\perp$;

(5) si consideri la proiezione ortogonale π_ε di V sul sottospazio V_ε di dimensione n, definita come

$$\pi_\varepsilon f := \sum_{i=1}^{n} \langle f, \varphi_i \rangle \varphi_i.$$

Allora $\pi_\varepsilon(V_\varepsilon^\perp) = \{0\}$.

Dimostrazione. Per il primo enunciato è sufficiente constatare che se φ è una funzione caratteristica di $\mathscr{K}$, allora $\mathscr{K}(R_y\varphi) = R_y(\mathscr{K}\varphi) = R_y(\lambda\varphi) = \lambda R_y\varphi$. Il secondo segue dalle precedenti proprietà (a) e (b) per quanto riguarda la finitezza della dimensione e da (1) per quanto concerne la seconda parte.

Per il terzo punto, sia $\{\varphi_1, ..., \varphi_n\}$ una base per V_ε, che esiste finita per (2). Se ora si considera $f \in V$, allora

$$f = \left(\sum_{i=1}^{n} \langle f, \varphi_i \rangle \varphi_i\right) + \left(f - \sum_{i=1}^{n} \langle f, \varphi_i \rangle \varphi_i\right) = f_{V_\varepsilon} + f_{V_\varepsilon^\perp}$$

ove f_{V_ε} è il membro contenuto nella prima parentesi, mentre $f_{V_\varepsilon^\perp}$ è il membro contenuto nella seconda. Questo mostra effettivamente che $V = V_\varepsilon \oplus V_\varepsilon^\perp$. In

[9] $f \in V_\varepsilon^\perp \Leftrightarrow \langle f, g \rangle = 0, \forall g \in V_\varepsilon$.

particolare, $V_\varepsilon^\perp$ dovrà avere dimensione infinita.

Il passo successivo consiste nell'osservare che $\langle Ag, f\rangle = \langle g, A^t f\rangle$ per ogni applicazione lineare $A : \mathbb{R}^n \to \mathbb{R}^n$; quindi si dovrà avere anche che $A : V_\varepsilon^\perp \to V_\varepsilon^\perp$; infatti, se $f \in V_\varepsilon^\perp$, allora $\langle Af, g\rangle = \langle f, A^t g\rangle = 0$ per ogni $g \in V_\varepsilon$, poiché $Ag \in V_\varepsilon$; dunque $Af \in V_\varepsilon^\perp$. Così, per invarianza dell'integrale di Haar, si può osservare che $\langle R_y g, f\rangle = \langle g, R_{y^{-1}} f\rangle$ e quindi anche R_y preserva $V_\varepsilon^\perp$, cioè lo mappa in sè stesso.

L'ultimo punto è banale. $\square$

In più, analogamente al Lemma 4.3.5, si possono mostrare i seguenti risultati:

1. $\pi_\varepsilon \circ R_y = R_y \circ \pi_\varepsilon$;

2. $\pi_\varepsilon \circ A = A \circ \pi_\varepsilon$;

3. se h è tale che $h(yxy^{-1}) = h(x)$, allora $\pi_\varepsilon \circ L_y = L_y \circ \pi_\varepsilon$.

Dimostrazione. Per la prima di queste relazioni si osservi innanzitutto che R_y è un endomorfismo di V_ε che trasforma funzioni caratteristiche in funzioni caratteristiche degli stessi autovalori. Dunque, se $\varphi_1, ..., \varphi_n$ è una base ortonormale di V_ε, visto che $\langle R_y\varphi_i, R_y\varphi_j\rangle = \langle\varphi_i, \varphi_j\rangle$, anche $R_y\varphi_1, ..., R_y\varphi_n$ è una base ortonormale dello stesso spazio. Pertanto

$$\pi_\varepsilon f = \sum_{i=1}^{n} \langle f, \varphi_i\rangle\varphi_i = \sum_{i=1}^{n} \langle f, R_y\varphi_i\rangle R_y\varphi_i \tag{4.3.5}$$

Ora non resta che osservare che

$$(R_y(\pi_\varepsilon f))(x) = \sum_{i=1}^{n} \langle f, \varphi_i\rangle R_y\varphi_i(x) = \sum_{i=1}^{n} \left(\int f(z)\varphi_i(z)dz \right)\varphi_i(xy)$$

sulla base $\varphi_1, ..., \varphi_n$, mentre su $R_y\varphi_1, ..., R_y\varphi_n$ si può scrivere

$$\begin{aligned}(\pi_\varepsilon(R_y f))(x) &= \sum_{i=1}^{n} \langle R_y f, R_y\varphi_i\rangle R_y\varphi_i(x) = \sum_{i=1}^{n} \left(\int f(zy)\varphi_i(zy)dz \right)\varphi_i(xy) = \\ &= \sum_{i=1}^{n} \left(\int f(z)\varphi_i(z)dz \right)\varphi_i(xy)\end{aligned}$$

e in virtù di (4.3.5) questi due risultati possono essere combinati, ottenendo alfine la prima relazione. Analogamente si procede per la seconda, in quanto il Lemma 4.3.5 permette di affermare che anche A mappa funzioni caratteristiche in funzioni caratteristiche con lo stesso valore caratteristico e quindi $\langle A\varphi_i, A\varphi_j\rangle = \langle\varphi_i, \varphi_j\rangle$. Per la terza relazione, invece, si osservi che si può affermare che $\langle L_y\varphi_i, L_y\varphi_j\rangle = \langle\varphi_i, \varphi_j\rangle$ solo nelle ipotesi del Lemma 4.3.5, poiché questa uguaglianza è deducibile solo dalla commutatività di L_y e $\mathscr{K}$, la quale si verifica sotto le condizioni del suddetto lemma. Sotto tale ipotesi, *mutatis mutandis*, si procede come sopra. $\square$

Dopo la seguente e ultima definizione

Definizione 4.3.3. *Siano $\phi : G \to GL(V)$ una rappresentazione lineare di G e $v \in V$; l'insieme*

$$G_v := \{g \in G \,|\, \phi(g)v = v\}$$

è detto essere sottogruppo di isotropia *di G in v* [10].

si è ora pronti per provare il risultato cruciale di questo capitolo, che garantisce l'esistenza di speciali rappresentazioni lineari di gruppi compatti e dal quale seguirà come semplice corollario la risoluzione in positivo del quinto problema di Hilbert nel caso compatto, sulla falsariga della strategia adottata da von Neumann.

Teorema 4.3.3. *Siano G un gruppo compatto, H un suo sottogruppo chiuso e U un intorno dell'unità. Allora esiste una rappresentazione lineare $\phi : G \to GL(n, \mathbb{R})$ per qualche $n \in \mathbb{N}$ ed esiste $v \in \mathbb{R}^n$ tali che $H \subset G_v \subset UH$.*

Dimostrazione. Ricordando la proprietà (6) di cui gode qualsiasi gruppo topologico, si può scegliere un intorno aperto simmetrico W dell'unità tale che $W^2 \subset U$. Sia inoltre $h : G \to \mathbb{R}$ una funzione continua non negativa tale che

1. $h(e) = 1$;
2. $h(x^{-1}) = h(x)$;
3. $h(x) = 0$ per $x \notin W$.

Una tale funzione esiste per il seguente motivo: per il lemma di Urysohn[11] certamente esiste una funzione continua $q : G \to \mathbb{R}$ non negativa tale che $q(e) = 1$ e q si annulla all'esterno di W, cioè $q(x) = 0$ per $x \in G \setminus W$; di conseguenza, la seguente mappa

$$h(x) := \frac{1}{2}[q(x) + q(x^{-1})]$$

è quella cercata, in quanto soddisfa tutte le precedenti proprietà. Si può allora definire il ben noto operatore $\mathscr{K}$ come in (4.3.1) con $k(x, y) = h(xy^{-1})$. Se in più si considera G/H, allora tale spazio quoziente è ancora compatto e di

[10] Si verifica facilmente che è un sottogruppo chiuso di G, perché per definizione ϕ è continua e quindi se $\{g_n\}_{n\in\mathbb{N}} \subset G_v$ è una successione convergente a g, allora $\phi(g_n) \to \phi(g)$. Di conseguenza, anche $\phi(g)v = v$.

[11] Tale lemma afferma che se X è uno spazio topologico, allora sono equivalenti le seguenti affermazioni:

(a) se A è un insieme chiuso e non vuoto di X, allora ogni intorno U di A contiene un intorno chiuso di A;

(b) se A, B sono insiemi chiusi e disgiunti di X, allora esiste una funzione continua $f : X \to [0, 1]$ tale che $f(x) = 0$ se $x \in A$, mentre $f(x) = 1$ se $x \in B$.

Nella dimostrazione in esame è verificata l'asserzione (a), che permette di dedurre (b), perché uno spazio compatto di Hausdorff è normale (cioè è T_1 e, comunque presi due chiusi disgiunti, esistono due loro intorni a loro volta disgiunti).

Hausdorff, dunque normale;[12] perciò, sempre per il lemma di Urysohn esiste una funzione non negativa $\tilde{f} : G/H \to \mathbb{R}$ tale che $\tilde{f}(eH) = 1$ e $\tilde{f}(xH) = 0$ per $x \notin WH$. Questo giustifica la definizione della funzione $f : G \to \mathbb{R}$ come $f(x) := \tilde{f}(xH)$: questa, pure non negativa, è ovviamente tale che $f(e) = 1$ e $f(x) = 0$ per $x \notin WH$, poiché eredita queste proprietà da $\tilde{f}$. In più, per ogni $y \in H$, $R_y f = f$.

Sia $g = \mathscr{K} f$. Per il Lemma 4.3.5, R_y e $\mathscr{K}$ commutano, dunque $R_y g = g$ per ogni $y \in H$. Si osservi poi che non può essere $g \equiv 0$, perché se $g(x) = 0$ per ogni $x \in G$, allora per la proprietà 5. della Definizione 3.2.1 $h(xy^{-1})f(y) = 0$ per ogni $x, y \in G$, dunque in particolare anche per $y = e$. Ma in tal caso, visto che $f(e) = 1$, allora $h(x) = 0$ per ogni $x \in G$, il che non può però verificarsi, visto che $h(e) = 1$. Di conseguenza esiste almeno un $x \in G$ tale che $g(x) \neq 0$ e, visto che in tal caso la funzione integranda non è identicamente nulla, allora per qualche $y \in G$ si dovrà avere $xy^{-1} \in W$ (perché così $h(xy^{-1}) \neq 0$) e $y \in WH$ (perché così $f(y) \neq 0$); in questo modo $x \in Wy \subset W^2H \subset UH$ e, per contronominale, se $x \notin UH$, allora $g(x) = 0$. Infine $g(e) > 0$ perché la funzione integranda, che è continua, non è identicamente nulla (per esempio per $y = e$).

A questo punto, ricordando la precedente proprietà (c) di cui gode l'operatore $\mathscr{K}$, si può affermare che $\pi_\varepsilon g \to g$ uniformemente per $\varepsilon \to 0$, perché così, volgarmente, V_ε "tende" a V, in quanto la sua dimensione cresce grazie all'aggiunta delle funzioni caratteristiche associate ai nuovi valori carattersitici di cui si deve tenere conto al diminuire di ε, e di conseguenza la proiezione di g su V_ε si traduce in quella che non è più una proiezione, ma è semplicemente la scrittura di g sulla base di V data dalle funzioni caratteristiche. Più formalmente, $\pi_\varepsilon g = \sum_{i=1}^{n} \langle g, \varphi_i \rangle \varphi_i$ e per $\varepsilon \to 0$ si ha che $n \to \infty$: la prova della convergenza uniforme segue dal Teorema 4.3.2. Per questo motivo, si può scegliere ε sufficientemente piccolo, in modo tale che

$$R_x \pi_\varepsilon g(e) = \pi_\varepsilon g(x) < \pi_\varepsilon g(e), \quad \forall x \in G \setminus UH$$

e ciò è vero, in quanto come detto poc'anzi $g(x) < g(e)$ per $x \in G \setminus UH$. Per lo stesso valore di ε si definisca $v := \pi_\varepsilon g \in V_\varepsilon$. Allora si può considerare l'azione di G sullo spazio vettoriale V_ε, che ha dimenione finita, attraverso R_x. In questo modo si può osservare che

$$R_x v \neq v, \quad \forall x \notin UH$$

in quanto, per costruzione (o meglio per scelta di ε), differiscono precisamente nell'unità, cioè $R_x v(e) \neq v(e)$. D'altra parte

$$R_y v = v, \quad \forall y \in H$$

poiché R_y commuta con π_ε. Si è così provato che il sottogruppo di isotropia di G in v contiene H ed è contenuto in UH, che è quanto ci si era prefissati.

[12] Per la Proposizione 1.4 di [9], infatti, se H è un sottogruppo chiuso di G, allora G/H è di Hausdorff in quanto spazio topologico, ma non si può dire nulla di particolare sulla sua struttura di gruppo. Se invece H è un sottogruppo chiuso normale, allora per la Proposizione 1.5 dello stesso testo G/H è un gruppo topologico.

Forse è superfluo evidenziare come la rappresentazione lineare ϕ richiesta dall'enunciato sia data dalla traslazione a destra $R_{(\cdot)}$. Per quanto già osservato precedentemente, infatti, $R_{(\cdot)}$ rappresenta G con endomorfismi dello spazio vettoriale infinito-dimensionale V, ma nel contesto della dimostrazione in corso tali endomorfismi possono essere ristretti a V_ε, che ha invece dimensione finita, sia n. Ne segue che $R_x \in \mathrm{Hom}(V_\varepsilon, V_\varepsilon)$ e poiché $\mathrm{Hom}(V_\varepsilon, V_\varepsilon)$ è isomorfo a $\mathcal{M}(n \times n, \mathbb{R})$, allora a R_x può essere associata una matrice quadrata di ordine n. Essa è in più non singolare perché R_x è un isomorfismo e quindi si conclude. $\square$

Alternativamente, la dimostrazione può essere specializzata e finalizzata alla dimostrazione del corollario successivo, assumendo che $H = \{e\}$.

Dimostrazione. Innanzitutto in questo caso la dimostrazione si riduce a provare che $G_v \subset U$, in quanto G_v è un sottogruppo di G e dunque certamente $e \in G_v$.

Per quanto già esposto precedentemente esiste un intorno aperto simmetrico W dell'unità ed esiste una funzione $h : G \to \mathbb{R}$ con le suddette proprietà, che consente di definire l'operatore $\mathscr{K}$ rispetto alla funzione nucleo $k(x,y) := h(xy^{-1})$. Inoltre, poiché $\{e\}$ è chiuso ed è banalmente un sottogruppo normale di G, allora G è normale come spazio topologico e per il lemma di Urysohn esiste una funzione non negativa $f : G \to \mathbb{R}$ tale che $f(e) = 1$ e $f(x) = 0$ per $x \notin W$. Come sopra si ponga $g := \mathscr{K} f$. Allora non può essere $g \equiv 0$ e quindi esiste $x \in G$ tale che $g(x) \neq 0$; questo permette di dire, visto che la funzione integranda non è identicamente nulla, che per qualche $y \in G$ si ha $xy^{-1} \in W$ (perché così $h(xy^{-1}) \neq 0$) e $y \in W$ (perché così $f(y) \neq 0$). Di conseguenza $x \in Wy \subset W^2 \subset U$ e quindi per contronominale $g(x) = 0$ se $x \notin U$; d'altra parte $g(e) > 0$.

Osservando ora che $\pi_\varepsilon g \to g$ per $\varepsilon \to 0$ per quanto già detto prima, si conclude constatando che per ε sufficientemente piccolo si ha $\pi_\varepsilon g(x) < \pi_\varepsilon g(e)$ per $x \in G \setminus U$, in quanto ciò è vero per g. In questo modo

$$R_x \pi_\varepsilon g(e) = \pi_\varepsilon g(x) < \pi_\varepsilon g(e), \quad \forall x \in G \setminus U$$

e ponendo $v := \pi_\varepsilon g \in V_\varepsilon$ segue che $R_x v \neq v$ per ogni $x \notin U$, cioè se $x \notin U$ allora non può nemmeno appartenere al sottogruppo di isotropia in v e questo conclude la dimostrazione. $\square$

Ne segue facilmente il prossimo corollario.

Corollario 4.3.1. *Siano G un gruppo compatto e U un intorno dell'unità in G. Allora esiste una rappresentazione $\psi : G \to GL(n, \mathbb{R})$ con $\ker \psi \subset U$.*[13]

Dimostrazione. Banale. Infatti, dal teorema precedente nel caso in cui $H = \{e\}$ segue che esistono una rappresentazione lineare $\psi : G \to GL(n, \mathbb{R})$ e $v \in \mathbb{R}^n$ tali

[13] In realtà si potrebbe provare un enunciato leggermente più forte, richiedendo che l'omomorfismo ψ sia a valori nel gruppo ortogonale; ciò è possibile, perché ogni rappresentazione di un gruppo compatto G su uno spazio vettoriale V di dimensione n è equivalente a una rappresentazione ortogonale di G su $\mathbb{R}^n$. A tal riguardo si può per esempio leggere [9] a pagina 14 per quanto riguarda il Teorema 3.5.

che $G_v \subset U$. A questo punto non resta che osservare che $\ker \psi \subset G_v$, perché se $g \in \ker \psi$, allora $\psi(g) = I$ e di conseguenza $\psi(g)v = v$. $\square$

4.4 Conclusione

A questo punto non resta che trarre le conclusioni, risolvendo il quinto problema di Hilbert nel caso compatto e in ipotesi di *no small subgroups property*, che sarà chiarita tra breve, appoggiandosi al fatto, provato da von Neumann nell'articolo *Über die analytischen Eigenschaften von Gruppen linearer Transformationen und ihrer Darstellungen* comparso nel 1929, che ogni sottogruppo chiuso di un gruppo lineare generale è un gruppo di Lie. Prima è però doveroso definire un concetto che è stato più volte richiamato e accennato nel corso di questa trattazione, ma solo in modo informale.

Definizione 4.4.1. *Sia G un gruppo topologico. Esso si dice un* gruppo di Lie *se esiste una carta locale (x, U) centrata in 0* [14] *tale che le operazioni di gruppo su tale intorno e rispetto a tali coordinate siano analitiche.*

Indi, è basilare la *no small subgroups property.*

Definizione 4.4.2. *Sia G un gruppo topologico. Esso* non ha sottogruppi piccoli *o verifica la* no small subgroups property (NSS property) *se esiste un intorno U dell'unità che non contiene sottogruppi non triviali, cioè diversi dal gruppo banale $\{e\}$.*

È chiaro allora che, al contrario, un gruppo G possiede sottogruppi piccoli se ogni intorno dell'unità contiene un sottogruppo proprio non banale. A questo punto non resta che mostrare il seguente risultato.

Teorema 4.4.1. *Un gruppo topologico compatto G verifica la* NSS property *se e solo se è isomorfo a un sottogruppo chiuso di un gruppo lineare generale.*

Dimostrazione. Si provino le due implicazioni:

- $\Rightarrow$ per il Corollario 4.3.1 esiste un omomorfismo di gruppi $\psi : G \to GL(n, \mathbb{R})$ con nucleo contenuto in un intorno fissato dell'unità (più precisamente, per ogni scelta dell'intorno vi è un omomorfismo con la suddetta proprietà). Poiché $\ker \psi$ è un sottogruppo di G, in particolare normale, e G verifica la *NSS property*, allora $\ker \psi$ è banale: ciò significa che ψ è iniettivo ed è quindi un isomorfismo sull'immagine, che si proverà ora essere chiusa. Osservando perciò che G è compatto e $GL(n, \mathbb{R})$ è di Hausdorff, allora si può affermare che ψ è anche un omeomorfismo sull'immagine e quindi G è a tutti gli effetti isomorfo a un sottogruppo chiuso di un gruppo lineare generale;

[14] Questo significa che U è un intorno dell'unità e $x : U \to W \subset \mathbb{R}^n$ per qualche $n \in \mathbb{N}$, con W aperto, è un omeomorfismo tale che $x(e) = 0$. Il limitarsi ad un solo intorno dell'unità consente comunque di estendere la richiesta di analiticità a qualsiasi carta locale di qualsiasi altro punto del gruppo, in virtù dell'omogeneità dei gruppi topologici.

$\Leftarrow$ in questo senso è sufficiente provare che $GL(n, \mathbb{R})$ non ha sottogruppi piccoli, poiché per isomorfismo tale proprietà risulterà vera anche per G. Si consideri allora un intorno convesso U di $0 \in \mathcal{M}(n \times n, \mathbb{R}) \cong \mathbb{R}^{n^2}$ tale che $\exp : 2U \to GL(n, \mathbb{R})$ sia un omeomorfismo tra $2U$ e un opportuno intorno di I in $GL(n, \mathbb{R})$ [15]: si ricordi infatti che qualunque sia la matrice $A \in \mathcal{M}(n \times n, \mathbb{R})$, la sua matrice esponenziale è invertibile, in virtù della Proposizione 4.2.2. Si supponga ora che $H \subset \exp(U)$ sia un sottogruppo di $GL(n, \mathbb{R})$ e che non sia triviale: di conseguenza esiste $I \neq B \in H$ e per proprietà dell'esponenziale si può considerare $0 \neq A \in U$ tale che $e^A = B$. Posto $k := \min\{k \in \mathbb{N}_{\geq 1} \,|\, 2^k A \notin U\}$, allora $2^k A \in 2U \setminus U$ e $B^{2^k} = e^{2^k A} \in \exp(2U) \setminus \exp(U)$. Ma per il fatto che H è un gruppo, ed è pertanto chiuso rispetto alla moltiplicazione, si dovrebbe anche avere $B^{2^k} \in H \subset \exp(U)$, che è una palese contraddizione. Quindi H è banale e $GL(n, \mathbb{R})$ verifica la *NSS property.*

□

Alla luce di questo fatto, risulta immediata la dimostrazione di un caso particolare del risultato di von Neumann a proposito del quinto problema di Hilbert.

Teorema 4.4.2. *Se G è un gruppo topologico compatto che verifica la* NSS property*, allora è un gruppo di Lie.*

Dimostrazione. Dal fatto che G verifica la *NSS property*, per il Teorema 4.4.1 esso è isomorfo a un sottogruppo chiuso di un gruppo lineare generale; ma in virtù del celebre risultato di von Neumann, che afferma che ogni sottogruppo chiuso di un gruppo lineare generale è un gruppo di Lie, allora si ha la conclusione. □

[15] Ciò è possibile in quanto l'esponenziale è la funzione inversa del logaritmo.

Appendice A

Biografie

Per corredare gli aspetti teorici fin qui trattati, ecco una cornice storica inerente le biografie dei principali matematici fin qui incontrati.[1]

A.1 Andrew Gleason

Figlio di Eleanor Theodalinda Mattei e Henry Allan Gleason, Andrew nacque a Fresno (California) il 4 novembre 1921 e dopo gli studi liceali, nel 1938 entrò all'Università di Yale, ove si laureò nel 1942. Subito dopo entrò nella marina degli Stati Uniti come crittografo, con il compito di decifrare i messaggi giapponesi, ma tale lavoro fu poi ripetuto durante la successiva guerra di Corea (1950-53). Nel 1946 venne accettato come *Junior Fellow* ad Harvard e una conseguenza di tale fatto fu che non dovette mai scrivere una tesi di dottorato; in compenso, negli anni successivi seguì numerosi corsi di matematica e iniziò a maturare il suo interesse per i problemi di Hilbert, in particolare per il quinto. Nel 1957 divenne professore ad Harvard e si ritirò dalla carriera accademica solo nel 1992.

Per quanto riguarda la sua attività di ricerca, l'*annus mirabilis* fu il 1949, in cui pubblicò gli articoli *Square roots in locally Euclidean groups*, *On the structure of locally compact groups* e *A note on locally compact groups*. L'anno successivo, al Congresso Internazionale dei Matematici a Cambridge (Massachusetts), Gleason schematizzò un possibile modo per fare breccia nelle mura del quinto problema di Hilbert, sottolineando l'importanza dei sottogruppi a un parametro in gruppi localmente euclidei. E fu infatti con la medesima strategia che nel 1952, nel celebre articolo *Groups without small subgroups*, Gleason contribuì, insieme ai lavori di Montgomery, Zippin e Yamabe, alla completa risoluzione in positivo del quinto problema di Hilbert. Questo notevole contributo alla matematica gli valse il *Newcomb Cleveland Prize*, ma la vita di Gleason fu costellata da molte altre onorificenze e incarichi prestigiosi, tra cui quello di presidente dell'*American Mathematical Society*. Morì il 17 ottobre 2008, in seguito a complicazioni mediche.

[1] Tratte da http://www.history.mcs.st-and.ac.uk/ e http://wikipedia.org

A.2 Alfred Haar

L'11 ottobre 1885 vide i natali a Budapest Alfred Haar, figlio di Ignatz Haar ed Emma Fuchs. Solo tredici anni prima, le città di Buda, Obuda e Pest si erano unificate, cosicchè il giovane Alfred potè crescere in una città che si stava rapidamente trasformando in un centro artistico e letterario. Al ginnasio, Haar mostrò particolare interesse per la chimica e solo nel 1903, quando vinse il primo premio Eötvös, decise che si sarebbe iscritto a corsi universitari di matematica. Nel 1904 si trasferì a Göttingen, dove successivamente avviò la propria attività di ricerca sotto la supervisione di Hilbert; nel 1909 ottenne anche il dottorato, con la tesi *Zur Theorie der orthogonalen Funktionensysteme* e immediatamente dopo divenne anche docente a Göttingen. A distanza di soli tre anni tornò in Ungheria per diventare docente a Kolozsvàr, ma gli sconvolgimenti della Prima Guerra Mondiale e il successivo breve periodo della Repubblica Sovietica di Ungheria mutarono profondamente lo scenario nazionale, in quanto i territori ungheresi vennero ridotti a un terzo e Kolozsvàr fu ceduta alla Romania. Di conseguenza, l'università fu costretta a trasferirsi e la nuova collocazione fu Szeged, dove Haar e Riesz fondarono quella che sarebbe poi divenuta la scuola omonima, uno dei più importanti centri matematici d'Europa. A conferma di questo notevole prestigio, nel 1930 Haar e Riesz diedero vita anche alla rivista *Acta Scientiarum Mathematicarum.*

Passando agli aspetti più inerenti la ricerca, Haar si occupò principalmente di analisi, in particolare di equazioni differenziali ordinarie, ma tra il 1917 e il 1919 il suo interesse per il calcolo delle variazioni lo portò a dimostrare il lemma che reca il suo nome e che applicò poi al problema di Plateau. Ciononostante, Haar è universalmente riconosciuto per i suoi lavori di analisi su gruppi; con l'articolo *Der Massbegriff in der Theorie der kontinuierlichen Gruppen* edito nel 1933, infatti, Haar mostrò l'esistenza di misure invarianti su gruppi localmente compatti, fatto che sarebbe poi stato utilizzato da von Neumann, Pontryagin e Weil. E un tale risultato ispirò ben presto versi di celebrazione.

> *Said a mathematician named Haar,*
> *"Von Neumann can't see very far.*
> *He missed a great treasure -*
> *they call it Haar Measure -*
> *poor Johnny's just not up to par."*

Nel 1931 il matematico ungherese ricevette un'onorificenza dall'Accademia Ungherese di Scienze, ma solo due anni dopo morì, il 16 marzo, a Szeged.

A.3 David Hilbert

Il 23 gennaio 1862, sotto lo stesso sole königsbergico di Immanuel Kant, nacque David Hilbert, forse il matematico più eminente e influente, insieme a Henri Poincarè, del XIX e XX secolo.

Dopo essersi diplomato, si iscrisse all'Università di Königsberg (oggi Kaliningrad, in Russia), ove nel 1885 ottenne il dottorato con Lindemann, discutendo la tesi *Über invariante Eigenschaften spezieller binärer Formen, insbesondere der Kugelfunktionen*[2]. In quegli stessi anni anche Hermann Minkowski frequentava la stessa università e i due matematici ebbero così modo di conoscersi e stringere una forte amicizia, che avrebbe poi influenzato i lavori di entrambi. La carriera accademica di Hilbert iniziò ancora nel 1886 come assistente, ma ben presto divenne professore a Königsberg e nel 1895 compì il salto di qualità, trasferendosi a Göttingen e assumendo la cattedra lasciata vacante da Heinrich Weber. Contemporaneamente all'avvio della sua brillante carriera, nel 1888 Hilbert diede alla luce il suo famoso *teorema della base*, il quale afferma che ogni anello di invarianti è finitamente generato. La tecnica dimostrativa utilizzata era però completamente innovativa, perché non costruttiva, e infatti all'epoca venne bollata come *teologia, non matematica*. Ciononostante il matematico tedesco portò avanti le sue idee, migliorandole in un successivo articolo, che comparve nei *Mathematische Annalen* e a riguardo del quale Klein ebbe a dire

> *I do not doubt that this is the most important work on general algebra that the Annalen has ever published.*

Oltre a ciò, nel *Zahlbericht* del 1897 Hilbert mostrò anche un profondo interesse per la teoria algebrica dei numeri, secondo forse solo al suo grande influsso sulla geometria, il più eminente in tutta la storia della matematica dopo Euclide e sintetizzato nei *Grundlagen der Geometrie*[3]. In questa opera si può ritrovare quella necessità di fondamenti assiomatici su cui costruire l'edificio solido della matematica, che sarebbe poi stata proposta ufficialmente come via maestra al Secondo Congresso Internazionale dei Matematici.

Il nome di Hilbert è chiaramente legato in modo indissolubile ai problemi che recano il suo nome, ma anche agli spazi di funzioni omonimi, ai quali Hilbert giunse, come raccontato da Irving Kaplansky, a causa del suo interesse per le equazioni integrali. In tutta la sua vita, uno dei più brillanti figli di Königsberg contribuì quindi a svariate discipline della matematica: dalla teoria degli invarianti all'analisi funzionale, dalle equazioni integrali al calcolo delle variazioni; e in più lasciò un solco indelebile nella fondazione del modo moderno di concepire e fare matematica. Per questo sono forse perfette le parole del suo primo studente Otto Blumenthal per ricordarlo.

> *In the analysis of mathematical talent one has to differentiate between the ability to create new concepts thate generate new types of thought structures and the gift for sensing deeper connections and underlying unity. In Hilbert's case, his greatness lies in an immensely powerful insight that penetrates into the depths of a question. [...] Insofar as the creation of new ideas is concerned, I would place Minkowski higher, and of the classical great ones, Gauss, Galois and*

[2] *Sulle proprietà invarianti di speciali forme binarie, in particolare le funzioni circolari.*
[3] Fondamenti della Geometria (1899)

Riemann. But when it comes to penetrate insight, only a few of the very greatest were the equal of Hilbert.

Si spense il 14 febbraio 1943 a Göttingen, la città che i grandi matematici tedeschi del suo tempo, prima dell'avvento del nazionalsocialismo, avevano trasformato nella patria mondiale della matematica.

A.4 Sophus Lie

Marius Sophus Lie nacque il 17 dicembre 1842 a Nordfjordeid, in Norvegia, terra che pochi decenni prima aveva visto la nascita di Niels Henrik Abel. Figlio del pastore luterano Johann Herman Lie e sesto di sette fratelli, Sophus frequentò la scuola primaria nella cittadina di Moss, nel sud-est del paese, dopodichè nel 1857 si iscrisse alla *Scuola privata di latino* nell'allora Christiania, oggi Oslo. Per problemi alla vista non potè avviarsi alla carriera militare e quindi per sei anni, dal 1859 al 1865, frequentò svariati corsi all'Università di Christiania, da matematica a botanica fino a zoologia, senza sceglierne uno in particolare per la tesi. Nel 1868, tuttavia, maturò il suo interesse per la geometria, in particolare per quella di Julius Plücker e Jean Victor Poncelot, e così l'anno seguente, sul *Journal für die reine und angewandte Mathematik*[4], apparve il suo primo articolo circa i numeri immaginari. Per tale motivo Lie vinse una borsa di studio, che gli permise di viaggiare ed entrare così in contatto con alcuni dei più importanti matematici dell'epoca, che allora si trovavano all'Università di Berlino: Leopold Kronecker (1823-1891), Ernst Eduard Kummer (1810-1893), Karl Weierstrass (1815-1897) e Felix Klein (1849-1925), le stesse personalità che di lì a pochi anni avrebbe incontrato anche Friedrich Schur.

In particolare Lie iniziò una proficua e profonda collaborazione con Klein, che influenzò notevolmente anche quest'ultimo. Infatti fu il matematico norvegese a presentare il concetto di gruppo a quello tedesco. Nel 1870 i due si recarono a Parigi, incontrando Jean Gaston Darboux, Michel Chasles, Camille Jordan e iniziando a lavorare ai gruppi di trasformazioni, ma nel luglio dello stesso anno, a causa dello scoppio della guerra franco-prussiana, Klein fu costretto a tornare a Berlino, mentre Lie venne arrestato e imprigionato a Fontainebleau, perché i suoi appunti matematici furono scambiati per messaggi cifrati di spionaggio. Liberato, nel 1872 tornò a Christiania per ottenere il dottorato con una tesi sulla teoria delle trasformazioni e divenire così professore. Nel 1882 fondò la rivista *Acta Mathematica* e nel 1886 ottenne la cattedra di matematica all'Università di Leipzig, sostituendo proprio Klein; ma l'integrazione nel nuovo ambiente fu difficile e questo lo condusse alla depressione, già latente e causata dall'assenza di riconoscimenti nella comunità matematica. Dopo essere diventato membro dell'*Accademia delle scienze francese* il 7 giugno 1872 e aver ricevuto il premio Lobacevskij nel 1897, l'anno seguente, malato, tornò a Christiania, dove si spense il 18 febbraio 1899 a causa di una anemia perniciosa.

Nel 1921 Friedrich Engel, allievo di Klein e Lie, e Paoul Heegaard pub-

[4] *Rivista per la Matematica Pura e Applicata.*

blicarono l'opera completa del matematico norvegese, intitolata *Gesammelte Abhandlungen*.

A.5 Deane Montgomery

Nato il 2 settembre 1909 a Weaver, in Minnesota, Deane Montgomery crebbe in una fattoria e frequentò la Hamline University di Saint Paul, la prima istituzione per alta educazione di tutto lo Stato del Minnesota. Lì si laureò, dopodichè si trasferì all'Università dell'Iowa per un master e per il dottorato, che conseguì nel 1933. La tesi interessava argomenti di topologia, gli stessi che sarebbero poi stati presenti nei suoi primi articoli. Nel 1933-34 Montgomery entrò nel Consiglio Nazionale di Ricerca ad Harvard, ma l'anno successivo optò per Princeton, trovando il nuovo ambiente estremamente piacevole. Nel 1935 iniziò a insegnare allo Smith College, mentre negli anni del secondo conflitto mondiale lavorò insieme a von Neumann sull'analisi numerica. Nel 1946 si trasferì a Yale, ma deluso dall'ambiente accademico tornò all'*Institute of Advanced Study* di Princeton, ove nel 1951 divenne professore. Lì rimase fino al 1980, quando si ritirò dall'insegnamento.

Dal punto di vista dell'attività di ricerca, si interessò particolarmente alla topologia algebrica e geometrica, ma brillò per il suo contributo allo studio dei gruppi di trasformazioni. Sull'argomento scrisse svariati articoli in collaborazione con Leo Zippin, come *Compact Abelian transformation groups* nel 1938 e *A theorem on Lie groups* nel 1942, per citarne un paio. E l'analisi dei gruppi di trasformazioni portò Montgomery a indagare sul quinto problema di Hilbert, riuscendolo a risolvere nel 1948 in dimensione 3 e nel 1952 con l'assunzione di dimensione finita, nello stesso anno in cui Yamabe divenne suo assistente. In virtù dei numerosi contributi resi alla matematica, Montgomery divenne dottore onorario in molte università statunitensi e rivestì incarichi di prestigio, come quello di vicepresidente dell'*American Mathematical Society* (1952-53) e poi di presidente (1961-62). Morì il 15 marzo 1992 a Chapel Hill, in North Carolina, e anche se lontano dagli studi e dalle università, non per questo dimenticato, perché aveva profondamente influenzato chi gli era stato vicino negli anni precedenti, come ricorda Armand Borel:

> *He was always seeking out and encouraging young mathematicians. He and his wife Kay would regularly and very warmly receive the visiting members at their home. Maybe remembering his own beginnings in an out of the way place, he had a special interest, and talent, in finding out people with considerable potential among some applicants from rather isolated places about whom not much was available.*

A.6 Lev Semenovich Pontryagin

Lev Pontryagin nacque il 3 settembre 1908 a Mosca; di umile estrazione, la sua famiglia non potè permettere al futuro matematico un'educazione adeguata alle sue potenzialità. Inoltre, ad aggravare ulteriormente la situazione, all'età di quattordici anni Lev rimase vittima di un'esplosione che lo rese cieco. Questo fatto avrebbe probabilmente potuto mettere fine all'educazione del giovane e ad ogni sua ambizione futura, se non fosse stato per lo straordinario sforzo della madre Tat'yana Andreevna, che lesse al figlio testi scientifici in svariate lingue e scrisse i suoi manoscritti senza aver ricevuto alcuna educazione. Si deve quindi riflettere su come, a volte, la gloria di un matematico non sia da ricercare solo nel talento individuale, ma anche in fattori esterni, come il contesto socio-politico o come in questo caso l'impegno di una persona senza alcuna preparazione matematica.

Nel 1925 Pontryagin entrò all'Università di Mosca e i suoi insegnanti notarono immediatamente il suo straordinario talento, che gli consentiva di "vedere" molto più lontano di tutti gli altri studenti. Inoltre il giovane Lev iniziò subito a frequentare corsi avanzati, avvicinandosi così ad Aleksandrov, che lo influenzò profondamente nei primi anni di ricerca. Infatti, a soli diciannove anni, Pontryagin aveva già prodotto risultati importanti sul teorema di dualità di Alexander. Nel 1929 si laureò e nel 1934 divenne un membro dell'Istituto Steklov, del cui Dipartimento di Toplogia e Analisi Funzionale fu nominato capo l'anno successivo. Ma ancora nel 1934, il matematico russo fu in grado di risolvere il quinto problema di Hilbert per gruppi abeliani localmente compatti, utilizzando la teoria dei caratteri da lui appositamente introdotta e nel 1938 scrisse [8], uno dei testi più significativi sull'argomento. Per quasi due decenni Pontryagin proseguì i propri studi in topologia, ma nel 1952 fece un cambio apparentemente drastico, indirizzandosi da quel momento fine alla fine dei suoi giorni alla matematica applicata: in particolare alle equazioni differenziali e alla teoria del controllo; come già detto, però, tale scelta fu solo apparentemente inaspettata, perché maturata in seguito alla conoscenza negli Anni Trenta del fisico A. Andronov. Negli anni successivi Pontryagin fu investito di numerose onorificenze da parte del governo sovietico, ma il suo prestigio era considerevole anche a livello internazionale, in quanto nel 1970 venne eletto vicepresidente dell'Unione Matematica Internazionale.

Si spense il 3 maggio 1988 nella sua città natale.

A.7 Friedrich Heinrich Schur

Friedrich Heinrich Schur nacque il 27 gennaio 1856 a Maciejewo (Polonia) e dopo il ginnasio, frequentato a Krotoschin, nel 1875 si iscrisse all'università di Breslau, iniziando a frequentare i corsi di astronomia. Tuttavia, l'influenza di Heinrich Schröter (1829-1892) e Jacob Rosanes (1842-1922) lo indirizzò ben presto verso la matematica e per questo, dopo tre semestri, Schur si trasferì a Berlino, dove all'epoca erano docenti matematici quali Leopold Kronecker (1823-1891), Ernst

Eduard Kummer (1810-1893) e Karl Weierstrass (1815-1897) e un fisico in particolare: Gustav Kirchhoff (1824-1887). Sotto l'egida di Kummer, con la tesi *Geometrische Untersuchungen über Strahlenkomplexe ersten und zweiten Grades* Schur, nel 1879, ottenne il dottorato e, a distanza di due anni, l'abilitazione con il lavoro *Über die durch kollineare Grundgebilde erzeugten Kurven und Flächen* presso l'università di Leipzig. Insegnò come docente privato fino a quando, nel 1884, divenne assistente di Felix Klein (1849-1925) e, l'anno successivo, professore a Leipzig. Iniziò così a interessarsi alla geometria proiettiva e riemanniana, divenendo noto per risultati quali il fatto che se in una varietà riemanniana di dimensione maggiore o uguale a tre tutti i punti sono isotropi, allora tale varietà ha curvatura costante[5]. Nel 1888 egli divenne professore di Matematica Pura all'università di Dorpat (Estonia), succedendo a Peter Helmling (1817-1901), e tale data è fondamentale, in quanto segnò l'inizio dell'interesse di Schur per i gruppi di trasformazioni continue, una nuova branca della geometria differenziale che si stava rapidamente sviluppando proprio in quegli anni. Successivamente si spostò da Aachen a Karlsruhe e contemporaneamente diede alcuni contributi significativi alle fondamenta della geometria, cui si stava interessando anche David Hilbert[6]. Dal 1909 al 1919 Schur insegnò presso l'università di Strassburg, dopodichè tornò a Breslau, ove spirò il 18 marzo 1932.

A.8 John von Neumann

John von Neumann, all'anagrafe Jànos Neumann, nacque il 28 dicembre 1903 a Budapest e il suo contributo è stato significativo in moltissimi ambiti: in teoria degli insiemi, analisi funzionale, topologia, fisica quantistica, economia, informatica, teoria dei giochi e fluidodinamica per citarne alcuni.

Di origine ebrea, discendente da una famiglia di banchieri, Janos Neumann si rivelò ben presto essere un *enfant prodige*, colpendo genitori e conoscenti con le sue rare doti di memoria, calcolo e padronanza delle lingue. A soli dieci anni, egli infatti conosceva già sei lingue, tra cui il greco antico. Nel 1911 entrò nel Ginnasio Luterano, ove la sua predisposizione alla matematica non passò inosservata e, anzi, venne coltivata, garantendo al giovane Janos un precettore privato universitario. Fu in questi anni che il matematico ungherese maturò una visione totalizzante della matematica, la quale, secondo von Neumann, poteva essere impiegata per trattare ogni aspetto delle relazioni sociali ed economiche. Ma gli eventi storici ebbero il sopravvento: nel 1919, l'instaurazione della Repubblica Sovietica Ungherese da parte di Bèla Kun constrinse la famiglia Neumann a emigrare in Austria; quando il regime comunista cadde, dopo soli cinque mesi, i Neumann tornarono in patria, ma dovettero far fronte alle persecuzioni antisemite del post-Kun.

Nel 1921 Janos Neumann completò gli studi presso il Ginnasio Luterano e già l'anno successivo pubblicò il suo primo lavoro in collaborazione con il pro-

[5] Friedrich H. Schur, *Über die Zusammenhang der Räume konstanten Riemannschen Krümmungmasses mit den projektiven Räumen*, Math. Ann. 27, pagg. 537-67 (1886)

[6] David Hilbert, *Grundlagen der Geometrie*, (1899)

prio precettore. Tuttavia il volere del padre era che Janos studiasse materie più "pratiche" (e non "teoriche" come la matematica). Per questo si raggiunse un compromesso: il futuro matematico si iscrisse all'Università di Budapest per studiare matematica, senza però frequentare le lezioni, e all'Università di Berlino per studiare chimica, ove rimase fino al 1923, anno in cui si trasferì a Zurigo. Nel 1926 si laureò in ingegneria chimica presso il Politecnico di Zurigo e ottenne anche il dottorato in matematica dall'Università di Budapest, discutendo una tesi di teoria degli insiemi. In questa egli fornì la definizione di numeri ordinali tuttora utilizzata. Nel periodo successivo si trasferì a Göttingen, ove sotto l'egida di David Hilbert iniziò ad interessarsi di fondamenti della matematica e di meccanica quantistica; contemporaneamente sviluppò la teoria dei giochi, pubblicando nel 1928 sui *Mathematische Annalen* l'articolo *Zur Theorie der Gesellschaftspiele*[7], contenente il noto *teorema di minimax*.

Dopo essere convolato a nozze con Marietta Kovesi, nel 1930 von Neumann fu invitato a Princeton, dove iniziò fin da subito a insegnare e nel 1933, quando fu fondato l'*Institute for Advanced Study*, divenne uno dei sei professori originari di matematica, insieme a J. W. Alexander, A. Einstein, M. Morse, O. Veblen e H. Weyl. A riguardo delle sue doti didattiche, tutto si riassume nei due seguenti commenti contrastanti, il secondo a riguardo della fisica.

> *His fluid line of thought was difficult for those less gifted to follow. He was notorious for dashing out equations on a small portion of the available blackboard and erasing expressions before students could copy them.*[8]
>
> *For a man to whom complicated mathematics presented no difficulty, he could explain his conclusions to the uninitiated with amazing lucidity. After a talk with him one always came away with a feeling that the problem was really simple and transparent.*[9]

Con l'avvento al potere del nazionalsocialismo in Germania, von Neumann, che aveva iniziato a farsi chiamare John, rifiutò ogni incarico universitario in terra tedesca e rimase così fino alla fine dei suoi giorni negli Stati Uniti. Al contrario di molti altri scienziati tuttavia, la sua posizione non fu mai quella di rifugiato politico e la sua popolarità a Princeton crebbe rapidamente e non solo per via della sua carriera nella ricerca, ma anche per i party che organizzava, per come sapeva intrattenere gli ospiti e per la sua giovialità.

Al di là di questo aspetto forse meno noto, fu invece vertiginosa per rilevanza la produzione scientifica del matematico ungherese. Nel 1944 infatti, durante la Seconda Guerra Mondiale, pubblicò insieme a Oskar Morgenstern il testo *Theory of Games and Economic Behavior*, in cui la teoria dei giochi, precedentemente abbozzata nel 1928, venne profondamente ampliata; tale scritto, alcuni anni più tardi, sarebbe stato uno dei punti di riferimento per Shannon. Nello stesso anno, nell'ambito del Progetto Manhattan per la realizzazione della

[7] *Sulla teoria dei giochi.*
[8] W. Poundstone, *Prisoner's dilemma*, Oxford (1993)
[9] Necrologio su *The Times.*

bomba atomica, venne a conoscenza dei primi tentativi di produrre macchine in grado di compiere centinaia di operazioni al secondo. Fu in quel momento che von Neumann iniziò a interessarsi anche alla teoria dell'informazione, nella quale lasciò il proprio contributo in quella che ancora oggi è nota come *architettura di von Neumann.*

Dal punto di vista politico, già nel 1937 John ebbe i primi contatti con le forze armate e da quell'anno il suo ruolo all'interno delle istituzioni politico-militari statunitensi subì un'escalation senza fine. All'interno del Progetto Manhattan rivestì un ruolo di primo piano, così come nello sviluppo della bomba al plutonio, mosso da un profondo sentimento antinazista e successivamente antisovietico. Proprio a causa del cosiddetto *pericolo rosso* von Neumann incentivò lo sviluppo di armi atomiche sempre più potenti e propose perfino di bombardare preventivamente l'Unione Sovietica; volle anche seguire di persona alcuni test preparatori per la bomba H (deflagrata nelle Isole Marshall nel 1952) e probabilmente fu in queste circostanze che si ammalò di tumore. Così, l'8 febbraio 1957, colpito da cancro alle ossa, John von Neumann si spense a Washington.

A.9 Hermann Weyl

Il 9 novembre 1885 a Elmshorn vide la luce Hermann Klaus Hugo Weyl, figlio di Anna Dieck e Ludwig Weyl. Dopo aver conseguito il proprio *Abiturarbeit*, nel 1904 entrò all'Università di Monaco, iniziando a seguire corsi sia di matematica sia di fisica; la stessa situazione perdurò anche quando si trasferì all'Università di Göttingen, dove subì l'enorme fascino di Hilbert. Sotto la supervisione di quest'ultimo, nel 1908, redasse la sua tesi di dottorato, dal titolo *Singuläre Integralgleichungen mit besonder Berücksichtigung des Fourierschen Integraltheorems*[10], mentre nel 1913 presentò la tesi di abilitazione *Über gewöhnliche Differentialgleichungen mit Singularitäten und die zugehörigen Entwicklungen willkürlicher Funktionen*[11], inerente la teoria spettrale di problemi singolari di Sturm-Liouville. Quest'ultimo lavoro divenne ben presto molto popolare, come *Die Idee der Riemannschen Fläche*, edito nel 1912, in cui per la prima volta comparvero la definizione di varietà differenziabile (sebbene solo 2-dimensionale) e la proprietà di separazione che sarebbe poi stata legata indissolubilmente al nome di Hausdorff. Per un breve periodo Weyl esercitò la professione di docente privato a Göttingen, ma dal 1913 al 1930 mantenne la cattedra alla *Zurich Technische Hochschule*, dove fino al 1914 fu collega di Einstein, il quale stava in quel momento sistemando i dettagli della relatività generale. Sfuggito alla coscrizione obbligatoria nell'esercito tedesco grazie a un permesso speciale del governo svizzero, Weyl tentò alcuni approcci innovativi alla relatività e nuovi sviluppi nella teoria di gauge, sebbene non apprezzati da Einstein, Pauli ed Eddington.

Nel 1921 Weyl strinse amicizia con Schrödinger, appena trasferitosi a Göttingen, mentre negli anni successivi sviluppò la teoria delle rappresentazioni di

[10] Equazioni integrali singolari
[11] Su equazioni differenziali ordinarie con singolarità

gruppi semisemplici, considerata da Weyl stesso uno dei suoi risultati più importanti. Tra il 1930 e il 1933 fu professore a Göttingen, occupando il posto lasciato vacante da Hilbert, ma gli avvenimenti politici del 1933, la salita al potere dei nazionalsocialisti e l'origine ebraica della moglie convinsero Weyl a trasferirsi a Princeton, all'*Institute for Advanced Study*, ove proseguì il suo interesse per le relazioni tra matematica e le avanguardie della fisica di allora, cioè relatività e meccanica quantistica. Fu nel 1951 che si ritirò dall'attività universitaria, per trascorrere la propria vita con la moglie a cavallo tra Princeton e Zurigo; tuttavia qui fu colto da un improvviso malore dopo essersi recato in posta per spedire delle lettere e il 9 dicembre 1955 morì.

Un aspetto forse meno noto di Weyl fu il suo interesse per la filosofia della matematica e per gli aspetti fondazionali della medesima; d'altra parte il matematico tedesco fu fortemente influenzato dalla filosofia di Edmund Husserl e la stessa moglie Helene Joseph era stata sua studentessa nel 1913.

A.10 Hidehiko Yamabe

Quinto figlio della famiglia Yamabe, Hidehiko nacque il 22 agosto 1923 ad Ashiya, nei pressi di Osaka. La sua vita fu sempre segnata dalle precarie condizioni di salute, tanto che ancora fanciullo il medico di famiglia aveva espresso il parere che difficilmente avrebbe superato i vent'anni di età. Dopo i primi livelli di istruzione, nel 1942 Yamabe si trasferì a Kyoto, in preparazione all'università, alla quale si iscrisse per studiare matematica nel 1944, nell'esatto momento in cui il martello della Seconda Guerra Mondiale stava per abbattersi con maggiore violenza sul Giappone. Laureatosi nel 1947, nel suo primo articolo dal titolo *On an arcwise connected subgroup of a Lie group* mostrò che un sottogruppo connesso per archi di un gruppo di Lie è un sottogruppo di Lie, dopodichè iniziò il proprio assedio al quinto problema di Hilbert, pur prestando particolare interesse agli altri ambiti della matematica. Così, parallelamente ad articoli come *On some properties of locally compact groups with no small subgroups* venivano pubblicati anche altri testi di topologia e gruppi topologici.

Nel 1952 Yamabe si trasferì negli Stati Uniti, ove ottenne un posto a Princeton come assistente di Deane Montgomery per due anni e in tale periodo pubblicò gli articoli *On the conjecture of Iwasawa and Gleason* e *A generalization of a theorem of Gleason*. Con questi il quinto problema di Hilbert veniva risolto in positivo. Nel 1954 il matematico nipponico inviò la propria tesi di dottorato all'Università di Osaka e nello stesso anno divenne professore presso l'Università del Minnesota. Fu in quel periodo che i suoi interessi si spostarono dai gruppi di Lie alle equazioni differenziali e alla geometria differenziale; infatti nel 1957 mostrò un modo alternativo ed elegante per costruire funzioni di Green per l'equazione del calore. Nel settembre del 1960 gli fu proposta una cattedra alla Northwestern University di Evanston, ma poco dopo aver accettato l'incarico morì, il 20 novembre, all'età di soli trentasette anni.

A.11 Leo Zippin

Nato il 25 gennaio 1905 a New York, Leo Zippin era figlio di immigrati ucraini di origine ebrea; il padre, Max Zippin, era in particolar modo legato alla cultura yiddish, tanto da scrivere numerosi pezzi teatrali in lingua, ma che non ebbero successo. Egli era inoltre di ispirazione socialista e per questo, quando nel 1917 scoppiò la Rivoluzione d'Ottobre in Russia, decise di partire insieme alla famiglia per essere testimoni di quella che riteneva sarebbe stata la realizzazione degli ideali marxisti. In realtà assistettero ad una realtà completamente diversa, fatta di povertà e guerra civile; per questo gli Zippin decisero di tornare negli Stati Uniti, ma poiché le comunicazioni a Occidente erano bloccate, dovettero muovere verso est, lungo la Trans-Siberiana. Una volta fatto rientro negli Stati Uniti, si stabilirono a Philadelphia, dove Leo potè riprendere la propria educazione, laddove interrotta. Nel 1922 entrò all'Università della Pennsylvania, dove era professore il topologo John Robert Kline, uno dei matematici più influenti nell'area di Philadelphia. Sotto la sua guida, Zippin completò gli studi e nel 1929 ottenne il dottorato di ricerca con la tesi *A study of continuous curves and their relation to the Janiszewski-Mullikin theorem.* Nonostante la Grande Depressione, che aveva ridotto drasticamente le possibilità di assunzione, Zippin ottenne dei contratti nazionali di ricerca presso l'Università del Texas e a Princeton, fino al 1933. Quando quell'anno il contratto terminò, la situazione lavorativa non era affatto migliorata, ma l'*Institute for Advanced Study* era appena stato fondato e a Zippin fu offerto un posto come assistente di James Alexander.

Nel 1934-35 vi fu un evento particolarmente significativo per la carriera e lo sviluppo matematico di Zippin, perché conobbe Deane Montgomery e i due divennero ben presto amici, intraprendendo una proficua collaborazione a distanza, perché poco tempo dopo Zippin si sarebbe trasferito a New York per insegnare al Queens College. Durante la Seconda Guerra Mondiale, troppo anziano per il servizio attivo, il matematico newyorkese si prestò volontario al Laboratorio di Ricerca Balistica e al termine del conflitto tornò lentamente alle attività precedenti, rinsaldando anche la collaborazione con Montgomery. Infatti nel 1952 i due pubblicarono tre articoli, che, insieme a un teorema di Andrew Gleason, mostravano come ogni gruppo localmente euclideo fosse un gruppo di Lie. In particolare, l'enunciato del teorema da loro dimostrato era il seguente:

> *Se G è un gruppo topologico separabile, metrico, localmente compatto, di dimensione finita, connesso e localmente connesso e se tutti i sottogruppi propri di G sono gruppi di Lie generalizzati, allora G contiene un sottogruppo di Lie generalizzato H chiuso e invariante tale che G/H ha dimensione finita e non ha sottogruppi piccoli.*

Leo Zippin si spense l'11 maggio 1995 a Manhattan.

Appendice B

Über die analytischen Eigenschaften von Gruppen linearer Transformationen und ihrer Darstellungen[1]

In questa appendice si passerà in esame il summenzionato articolo di von Neumann, edito nel 1929, presentando un breve estratto del contenuto e soffermandosi poi in particolare su quanto concerne la rappresentazione lineare di gruppi compatti, che, pur non essendo necessaria per la dimostrazione del fatto che ogni sottogruppo chiuso di un gruppo lineare generale è di Lie (per questo si sfruttano le proprietà della funzione logaritmo), è tuttavia un argomento particolarmente significativo.

B.1 Estratto

Come sottolineato dallo stesso von Neumann, il fine ultimo dell'articolo è quello di indagare e rendere più chiaro il ruolo giocato dalle ipotesi di continuità, differenziabilità e analiticità nella teoria dei gruppi continui di trasformazioni lineari, concetto che, come già detto, sarebbe stato reso più astratto e generale con l'introduzione dei gruppi di Lie solo successivamente. A tal fine si analizzano le rappresentazioni lineari, dipendenti da un certo numero di parametri analitici, dei sottogruppi normali di dati gruppi di matrici e in particolare le rappresentazioni che si instaurano tra un gruppo assegnato e il suo "gruppo infinitesimale", che con una terminologia più moderna è noto come algebra di Lie del gruppo in questione. In questo contesto, delle speciali rappresentazioni sono date dalle funzioni esponenziale e logaritmo, di cui si evidenziano alcune

[1] Sulle proprietà analitiche di gruppi di trasformazioni lineari e delle loro rappresentazioni, cfr. [14].

proprietà rilevanti. Successivamente, dopo aver visto come definire il gruppo infinitesimale per un qualsiasi gruppo di matrici a coefficienti reali o complessi, attraverso un processo di limite che ben giustifica l'aggettivo "infinitesimale", e aver indagato il numero di parametri atto a rappresentarlo, si giunge al primo seguente risultato, cercando di essere il più fedele possibile al lessico utilizzato nell'articolo.

Teorema B.1.1. *Sia $\mathfrak{G}$ un gruppo di matrici nello spazio euclideo $\mathcal{M}(n\times n,\mathbb{C})$.*[2] *Allora il suo gruppo infinitesimale $\mathfrak{I}$ è una varietà lineare; ciò significa che esistono k matrici $\overline{U_1},...,\overline{U_k}$ linearmente indipendenti, con $0 \leq k \leq 2n^2$, tali che $\mathfrak{I}$ è l'insieme delle combinazioni lineari a coefficienti reali di tali matrici, ovvero*

$$\alpha_1\overline{U_1} + \alpha_2\overline{U_2} + ... + \alpha_k\overline{U_k}, \quad \alpha_1,...,\alpha_k \in \mathbb{R}$$

Inoltre, se le matrici U, V appartengono a $\mathfrak{I}$, allora vi appartiene anche il loro commutatore $UV - VU$.

La componente connessa dell'unità in $\overline{\mathfrak{G}}$, denotata con $\overline{\mathfrak{G}}(e)$, è un sottogruppo normale di $\overline{\mathfrak{G}}$, che indica l'involucro di $\mathfrak{G}$.[3] *Analogamente, la componente connessa in $\overline{\mathfrak{G}}$ di un elemento g del gruppo, indicata con $\overline{\mathfrak{G}}(g)$, è la classe laterale di $\overline{\mathfrak{G}}(e)$ relativa a g, cioè $g\overline{\mathfrak{G}}(e)$.*

Ogni componente $\overline{\mathfrak{G}}(g)$ è aperta in $\overline{\mathfrak{G}}$ relativamente alla topologia indotta; di conseguenza il gruppo quoziente $\overline{\mathfrak{G}}/\overline{\mathfrak{G}}(e)$ è discreto: per nessuna matrice A con determinante non nullo possono esserci, a distanza piccola a piacere, infinite componenti distinte di $\overline{\mathfrak{G}}$.

Due matrici $A, B \in \overline{\mathfrak{G}}$ appartengono alla stessa componente di $\overline{\mathfrak{G}}$ se e solo se possono essere collegate da una curva analitica che giace interamente in $\overline{\mathfrak{G}}$.

$\mathfrak{G}(A)$ è l'insieme di tutte le matrici della forma $A \cdot \exp(U_1) \cdot \exp(U_2) \cdot ... \cdot \exp(U_j)$ con $U_1, ..., U_j \in \mathfrak{I}$. Ma ogni matrice $A \in \overline{\mathfrak{G}}$ possiede un intorno $\mathfrak{U}$ tale che la parte di $\overline{\mathfrak{G}}$ (oppure di $\overline{\mathfrak{G}}(A)$, che in questo contesto è lo stesso) che giace in esso[4] *è interamente descritta da $A \cdot \exp(U)$ al variare di $U \in \mathfrak{I}$, dato che la rappresentazione*

$$Y = \log(A^{-1}X), \quad X = A\exp(Y)$$

mappa in modo biunivoco $\mathfrak{U}$ in un certo intorno $\mathfrak{B}$ di $0 \in \mathfrak{I}$.[5] *Inoltre $\overline{\mathfrak{G}}$ può essere parametrizzato localmente in modo biunivoco e analitico con k parametri*

[2] Poiché, come di consueto, il gruppo è sottointeso essere moltiplicativo (e dunque l'operazione di gruppo è l'usuale prodotto di matrici), allora sarebbe più preciso asserire $\mathfrak{G} \subset GL(n,\mathbb{C})$.

[3] È costituito da $\mathfrak{G}$ stesso e da tutte le matrici che sono punti di accumulazione di successioni in $\mathfrak{G}$ e hanno in più determinante non nullo.

[4] Infatti non è inteso che $\mathfrak{U} \subset \overline{\mathfrak{G}}$ e quindi con l'espressione utilizzata si vuole indicare $\mathfrak{U} \cap \overline{\mathfrak{G}}$.

[5] Quanto si sta dicendo è che, mentre per una rappresentazione globale di $\mathfrak{G}(A)$ tramite esponenziale si necessita di un numero non meglio precisato di matrici appartenenti al gruppo infinitesimale di $\mathfrak{G}$, una rappresentazione locale della forma $A \cdot \exp U$ è invece sempre possibile. Ciò significa che esiste un opportuno intorno $\mathfrak{U}$ di A che è isomorfo a un certo intorno $\mathfrak{B}$ di $0 \in \mathfrak{I}$ attraverso $Y = \log(A^{-1}X)$ e $X = A\exp(Y)$.

reali;[6] *esso consta in* $\mathfrak{U}$ *di elementi della seguente forma*

$$A \cdot \exp(\alpha_1 \overline{U_1} + ... + \alpha_k \overline{U_k}), \quad (\alpha_1, ..., \alpha_k) \in \mathbb{R}^k \textit{ in un intorno di } (0, ..., 0).$$

Dopo questo risultato fondamentale, che, pur discutendo in generale le proprietà di un generico gruppo di matrici, anche in relazione con il gruppo infinitesimale ad esso associato, pone notevole enfasi sulle rappresentazioni del gruppo stesso tramite esponenziale e logaritmo[7], i paragrafi rimanenti dell'articolo sono imperniati sulle rappresentazioni continue del gruppo $\mathfrak{G}$ e su quella che viene chiamata "rappresentazione infinitesimale". Si osserva infatti che non necessariamente una rappresentazione di $\mathfrak{G} \subset \mathcal{M}(n \times n, \mathbb{R})$ in $\mathcal{M}(m \times m, \mathbb{R})$, che sia anche un omomorfismo di gruppi è continua, ma si individua una condizione (che in appendice si mostra non poter essere indebolita) sufficiente affinché ciò accada. E in tal caso non si prova la sola continuità, ma anche numerose altre proprietà analitiche, come la lipschitzianità. Per quanto riguarda invece la cosiddetta "rappresentazione infinitesimale", essa costituisce in qualche modo un "sollevamento" (non nel senso tecnico del termine) di una rappresentazione D tra gruppi di matrici $\mathfrak{G} \subset \mathcal{M}(n \times n, \mathbb{R})$ e $\mathrm{Im}(D) =: \mathfrak{H} \subset \mathcal{M}(m \times m, \mathbb{R})$ [8] alle rispettive algebre di Lie; in questo modo si costruisce un ponte non solo tra i due gruppi in questione, ma anche tra i rispettivi spazi tangenti nell'unità. Quanto provato in questi paragrafi è riassunto dalla seconda proposizione dell'articolo.

Teorema B.1.2. *Se D è una rappresentazione di $\mathfrak{G}$, che in un intorno dell'unità ha un'oscillazione minore di 1* [9] *(e questo è certamente il caso, se D non è ovunque discontinua), allora è continua in ogni punto di $\mathfrak{G}$ e può essere estesa in modo unico con continuità a $\overline{\mathfrak{G}}$.*

Tale estensione è una rappresentazione di $\overline{\mathfrak{G}}$ continua in tutto $\overline{\mathfrak{G}}$, soddisfa la condizione di Lipschitz in ogni sottoinsieme chiuso e limitato di $\overline{\mathfrak{G}}$ ed è ovunque infinitamente differenziabile. Può inoltre essere sviluppata su di un intorno di una certa matrice $A_0 \in \overline{\mathfrak{G}}$ in serie di potenze convergente nelle parti reali e immaginarie (se si considerano matrici complesse) degli ingressi dell'argomento.

Per questo motivo, nel caso complesso, non segue alcuna analiticità nel senso comune del termine, che è quello fornito dalle condizioni di Cauchy-Riemann. È infatti sufficiente considerare il gruppo delle trasformazioni lineari complesse

[6] Infatti, per quanto discusso nella nota precedente, $\mathfrak{U}$ è descritto interamente da $A \cdot \exp(U)$, ma ogni matrice $U \in \mathfrak{I}$ può essere espressa come combinazione lineare di al più k matrici linearmente indipendenti, ottenendo così una rappresentazione a k parametri di $\mathfrak{U}$.

[7] Si presti però attenzione al fatto che tali applicazioni non sono rappresentazioni lineari, in quanto non verificano la proprietà di gruppo.

[8] Il gruppo $\mathfrak{H}$, non presente nell'articolo originale, è un'introduzione puramente notazionale, per poter esprimere più chiaramente alcuni fatti successivi.

[9] Ovvero esistono $\delta > 0$ e $\eta > 0$ tali che, se $\|A - I\| < \delta$, allora $\|D(A) - D(I)\| < 1 - \eta$, ove $\|\cdot\|$ è l'ordinaria distanza euclidea dalla matrice nulla 0, definita come

$$\|A\| := \sqrt{\sum_{i,j=1}^{n} |a_{ij}|^2}.$$

invertibili: esso ammette, tramite il valore assoluto del determinante, una rappresentazione non analitica.

Infine, l'ultimo paragrafo è devoto alla presentazione di alcuni controesempi, presentati al termine da von Neumann per non interrompere il testo.

B.2 Sulla rappresentazione lineare di gruppi compatti

Si tratta ora di analizzare più nel dettaglio l'utilizzo che viene fatto da von Neumann delle rappresentazioni lineari di gruppi compatti. A tal fine ci si soffermerà sui paragrafi *IV. Darstellungen und Stetigkeit.*[10] e *V. Die Infinitesimaldarstellung und der Entwicklunssatz.*[11].

B.2.1 *Darstellungen und Stetigkeit*

Canonicamente, viene definita una rappresentazione di $\mathfrak{G} \subset \mathcal{M}(n \times n, \mathbb{R})$ in $\mathcal{M}(m \times m, \mathbb{R})$ come una funzione che soddisfa l'equazione funzionale $D(A \cdot B) = D(A) \cdot D(B)$ per ogni $A, B \in \mathfrak{G}$ e in più $D(I) = I^*$, ove I^* è la matrice identica di $\mathcal{M}(m \times m, \mathbb{R})$.[12] Queste due sole richieste non sono sufficienti per far sì che D sia anche continua, ma se in più essa ha oscillazione minore di 1 in un intorno di I, nel senso già discusso precedentemente, allora vale quanto enunciato nel Teorema B.1.2. In particolare, tale richiesta è certamente verificata se D è continua in I, ma non può essere indebolita, nel senso che esistono rappresentazioni con un'oscillazione pari a 2 in un intorno di I e che sono discontinue.[13]

Ma tornando al paragrafo in questione, ricorrendo alle proprietà di esponenziale e logaritmo di matrici, discusse e provate nel paragrafo *I. Die Funktionen exp und ln.*[14], von Neumann dimostra sotto la suddetta ipotesi che D è lipschitziana in un intorno di I e dunque continua. Il passo successivo è quello di mostrare che tale fatto vale in realtà globalmente su $\overline{\mathfrak{G}}$ e ciò viene fatto mostrando che D è lipschitziana su ogni compatto di $\overline{\mathfrak{G}}$. In questo modo si dimostra che D è una rappresentazione lineare di $\mathfrak{G}$ nel senso della Definizione 3.0.1 (cioè è anche continua) e segue anche la possibilità di estendere in modo unico D a $\overline{\mathfrak{G}}$, preservando la continuità e quindi la validità di $D(A \cdot B) = D(A) \cdot D(B)$: ciò significa che D è una rappresentazione lineare anche di $\overline{\mathfrak{G}}$. Inoltre l'estensione di D continua a verificare la proprietà di Lipschitz sui compatti di $\overline{\mathfrak{G}}$, ma la certezza di poter estendere in questo modo D sarebbe mal riposta se D non fosse continua su $\mathfrak{G}$ e infatti von Neumann fornisce un controesempio in tal senso.[15]

[10] IV. Rappresentazioni e continuità.

[11] V. La rappresentazione infinitesimale e la formula di sviluppo.

[12] In realtà questa seconda richiesta è implicitamente contenuta nella prima e la si può ricavare con minimo sforzo. Infatti $D(A) = D(A \cdot I) = D(A) \cdot D(I)$ e anche $D(A) = D(I \cdot A) = D(I) \cdot D(A)$ per ogni $A \in \mathfrak{G}$, il che significa che $D(I)$ è l'elemento neutro di $\mathcal{M}(m \times m, \mathbb{R})$, che è unico ed è I^*.

[13] cfr. [14], *Anhang* §1, esempio a).

[14] I. Le funzioni exp e ln.

[15] cfr. [14], *Anhang* §1, esempio b).

B.2.2 *Die Infinitesimaldarstellung und der Entwicklungssatz*

Nel paragrafo *II. Gruppen und ihre Infinitesimalgruppen.*[16], considerato un gruppo $\mathfrak{G}$ di matrici quadrate di ordine n e a coefficienti in $\mathbb{R}$, si è definito il suo gruppo infinitesimale $\mathfrak{I}$ come l'insieme di tutte le matrici $U \in \mathcal{M}(n \times n, \mathbb{R})$ per cui esistono una successione di matrici $\{A_k\}_{k\in\mathbb{N}} \subset \mathfrak{G}$ con $A_k \to I$ per $k \to \infty$ e una successione di numeri reali strettamente positivi $\{\varepsilon_k\}_{k\in\mathbb{N}}$ con $\varepsilon_k \to 0$ per $k \to \infty$ tali che

$$\lim_{k\to\infty} \frac{1}{\varepsilon_k}(A_k - I) = U$$

ove la convergenza è intesa essere puntuale nei singoli ingressi. La bellezza di questa definizione è insita nel fatto che permette di cogliere la natura analitica dell'algebra di Lie associata a un gruppo di matrici; infatti considerare quest'ultima come un'algebra equipaggiata con una forma bilineare antisimmetrica non consente di osservare come in realtà essa sia anche lo spazio tangente al gruppo di matrici nella matrice identica. Questo è invece reso evidente da von Neumann perché adotta un procedimento che richiama, per esempio, il modo in cui è naturale definire il vettore tangente a una curva parametrizzata. Si è poi provato facilmente che $\mathfrak{G}$ e $\overline{\mathfrak{G}}$ possiedono lo stesso gruppo infinitesimale.

Ora l'interesse è invece spostato sul seguente scenario

$$\begin{tikzcd}
\mathfrak{I} \arrow[r, "J_D"] \arrow[d, "\exp"] & \mathfrak{J} \arrow[d, "\exp^*"] \\
\overline{\mathfrak{G}} \arrow[r, "D"] & \overline{\mathfrak{H}}
\end{tikzcd}$$

Quella che nel paragrafo precedente era una generica rappresentazione D viene ora intesa come l'estensione a $\overline{\mathfrak{G}}$ della medesima rappresentazione, che deve essere dunque, in particolare, continua. Al di là di questa precisazione, assegnata la rappresentazione D, lo scopo delle ultime pagine dell'articolo è quello di indagare l'esistenza di J_D, che è la cosiddetta "rappresentazione infinitesimale" relativa a D. L'interrogativo è dunque il seguente: assegnati i gruppi di matrici $\overline{\mathfrak{G}}$ e $\overline{\mathfrak{H}}$, ai quali si possono associare i rispettivi gruppi infinitesimali $\mathfrak{I}$ e $\mathfrak{J}$, è possibile costruire $\mathfrak{J}$, attraverso la rappresentazione D, in termini di sole successioni di matrici appartenenti a $\overline{\mathfrak{G}}$? Se si riuscisse a rispondere affermativamente a tale quesito, si potrebbe poi constatare che tra D e J_D sussiste un rapporto fortemente analogo a quello presente tra una funzione tra varietà differenziabili e il suo differenziale.

Si prova innanzitutto che se le successioni $\{A_k\}_{k\in\mathbb{N}}$ con $A_k \in \overline{\mathfrak{G}}$ e $\{\varepsilon_k\}_{k\in\mathbb{N}}$ con $\varepsilon_k > 0$, $\varepsilon_k \to 0$ per $k \to \infty$ sono tali che

$$\frac{1}{\varepsilon_k}(A_k - I)$$

[16]II. Gruppi e loro gruppi infinitesimali.

sia convergente, allora anche

$$\frac{1}{\varepsilon_k}(D(A_k) - I^*)$$

lo è. Pertanto, se si fissa una matrice $U \in \mathfrak{J}$ e si considerano tutte le successioni $\{A_k\}_{k\in\mathbb{N}}$ con $A_k \in \overline{\mathfrak{G}}$ per cui esiste una successione $\{\varepsilon_k\}_{k\in\mathbb{N}}$ con le solite proprietà tale che

$$\lim_{k\to\infty} \frac{1}{\varepsilon_k}(A_k - I) = U,$$

allora anche tutte le successioni $\{\frac{1}{\varepsilon_k}(D(A_k)-I^*)\}_{k\in\mathbb{N}}$ convergono e hanno in più lo stesso limite, dipendente solo da U. Per tale motivo esso sarà indicato con $J_D(U)$ e, data l'arbitrarietà con cui è stata scelta $U \in \mathfrak{J}$, si può affermare che J_D è definita su tutto $\mathfrak{J}$. L'applicazione così individuata, come viene mostrato subito dopo, gode delle seguenti proprietà per ogni $U, V \in \mathfrak{J}$ e per ogni $\alpha \in \mathbb{R}$

$$\begin{aligned}
&J_D(\alpha U) = \alpha J_D(U) \\
&J_D(U + V) = J_D(U) + J_D(V) \\
&J_D(UV - VU) = J_D(U)J_D(V) - J_D(V)J_D(U)
\end{aligned}$$

Quindi, se le matrici $\overline{U_1}, ..., \overline{U_k}$ costituiscono una base di $\mathfrak{J}$, per cui ogni $U \in \mathfrak{J}$ può essere scritto in modo unico come $U = \alpha_1\overline{U_1} + ... + \alpha_k\overline{U_k}$ per $\alpha_1, ..., \alpha_k \in \mathbb{R}$, vale anche

$$J_D(U) = \alpha_1 J_D(\overline{U_1}) + ... + \alpha_k J_D(\overline{U_k})$$

Perciò $J_D(U)$ è lineare in U: in particolare è anche continua e infinitamente differenziabile. Ricordando come è stato scelto $\mathfrak{H}$, in modo tale che D risultasse suriettiva, si può allora effettivamente costruire $\mathfrak{J}$ a partire da $\overline{\mathfrak{G}}$ e D.

Infine, il paragrafo si chiude mostrando come $D(A)$, in un intorno di qualsiasi punto $A_0 \in \overline{\mathfrak{G}}$, sia sviluppabile in serie di potenze e che se $A \in \overline{\mathfrak{G}}$ appartiene a un intorno di I, allora $\log A \in \mathfrak{J}$.

Osservazione B.2.1. Dal paragrafo 2.16 di [12] sembrerebbe emergere come von Neumann si fosse già interessato a gruppi astratti localmente compatti nel presente articolo, ma dalla lettura non emerge alcun riscontro con questa asserzione. Tale fatto è corroborato dalle stesse parole dell'autore, che all'inizio del primo paragrafo, volendo trattare le funzioni esponenziale e logaritmo, fa riferimento al fatto che le trasformazioni lineari tra spazi vettoriali di dimensione n sono isomorfe alle matrici quadrate di dimensione n, mentre nell'incipit del secondo afferma

> *Als Gruppe bezeichnen wir, wie allgemein üblich, eine Menge in $\mathfrak{R}_m$ (d. h. eine Menge von Matrizen) $\mathfrak{G}$, die die folgenden Eigenschaften hat: [...] Als Infinitesimalgruppe $\mathfrak{J}$ von $\mathfrak{G}$ bezeichnen wir die Menge aller Matrizen U [...]*

Si ribadisce il concetto nel terzo paragrafo

> *Da die Gruppe* $\overline{\mathfrak{G}}$ *eine Punktmenge im euklidischen Raume* $\mathfrak{R}_m$ *ist, [...]*

e anche nel quarto si fa riferimento esclusivo a rappresentazioni di gruppi di matrici. Tutt'al più, una generalizzazione al caso localmente compatto si ha in [13], che è però uno scritto del 1933 e dunque successivo a quello trattato in questa sede.

Bibliografia

[1] David Hilbert, *Mathematical problems*, Bull. Amer. Math. Soc. 8, pp. 437-479 (1902)

[2] Ivor Grattan-Guinness, *A sideways look at Hilbert's twenty-three problems of 1900*, Notices of the American Mathematical Society

[3] Jeremy Gray, *The Hilbert problems 1900-2000*, Newsletter 36 European Mathematical Society (2000), pp. 10-13

[4] Ina Kersten, www.mathematik.uni-bielefeld.de/∼kersten/hilbert/problems.html

[5] Felix E. Browder, *Mathematical developments arising from Hilbert problems*, American Mathematical Society, Providence (1974)

[6] Deane Montgomery, *What is a topological group?*, The American Mathematical Monthly, Vol. 52, No. 6 (Jun. - Jul., 1945), pp. 302-307

[7] Karl H. Hofmann, Sidney A. Morris, *The structure of compact groups*, Walter de Gruyter, Berlin - New York

[8] Lev S. Pontryagin, *Topological Groups*, Gordon & Breach, Science Publishers Inc. (1938)

[9] Glen E. Bredon, *Introduction to compact transformation groups*, Volume 46 in Pure and Applied Mathematics, Academic Press (New York - London) (1972)

[10] John L. Kelley, T. P. Srinivasan, *Measure and Integral - Volume 1*, Springer Verlag (1988)

[11] Claude Chevalley, *Theory of Lie groups*, Princeton University Press (1946), pp. 206-210

[12] Deane Montgomery, Leo Zippin, *Topological transformation groups*, (1974), p.71

[13] John von Neumann, *Die Einführung analytischer Parameter in topologischen Gruppen*, Annals of Mathematics, 34, pp. 170-190 (1933)

[14] John von Neumann, *Über die analytischen Eigenschaften von Gruppen linearer Transformationen und ihrer Darstellungen*, Collected Works - Volume I, pp. 509-548 (1929)