Note di Teoria dei Numeri
A.A. 2019-20

Capitolo 1

Gruppi topologici

In questa sezione ricordiamo alcuni fatti riguardanti gruppi topologici.

Definizione 1.0.1 *Sia G un gruppo dotato di una topologia τ. Diremo che G è un* gruppo topologico *se le due applicazioni*

$$\begin{aligned} \iota : G &\longrightarrow G \\ g &\longmapsto g^{-1} \end{aligned} \qquad\qquad \begin{aligned} \mu : G \times G &\longrightarrow G \\ (g,h) &\longmapsto gh \end{aligned}$$

sono continue.

Esempi di gruppi topologici non sono difficicili da trovare.

- Ogni gruppo dotato della topologia discreta è un gruppo topologico.
- $\mathbb{R}^n$ con la topologia usuale è un gruppo topologico.
- Il gruppo $\mathbb{S}^1 = \{z \mid z \in \mathbb{C}\ |z| = 1\}$ con la topologia indotta da quella di $\mathbb{C}$ è un gruppo topologico.

Se G è un gruppo topologico ed N è un suo sottogruppo normale, è possibile definire una topologia nel gruppo quoziente G/N, in modo che la proiezione canonica $\pi : G \longrightarrow G/N$ risulti continua. Infatti, scegliendo $\mathcal{A} = \{A \subseteq G/N \mid \pi^{-1}(A) \text{ è aperto di } G\}$ come insieme di aperti, si vede immediatamente che π risulta continua e, inoltre, ogni topologia su G/N che renda continua π è contenuta in $\mathcal{A}$. Pertanto, nel contesto dei gruppi topologici, i quozienti vengono sempre pensati dotati di questa topologia, detta appunto la *topologia quoziente*. Come è facile intuire, gli usuali teoremi di omomorfismo hanno un loro corrispettivo *topologico*, la cui formulazione (ed eventuale dimostrazione) è lasciata al lettore.

Un esempio di applicazione del I Teorema di isomorfismo è il seguente.

Esempio Sia $\sigma : \mathbb{R} \longrightarrow \mathbb{C}^*$ la funzione definita da $\sigma(x) = e^{2\pi i x}$. I gruppi $(\mathbb{R}, +)$ e $(\mathbb{C}^*, \cdot)$ li pensiamo dotati delle loro usuali topologie. Si controlla immediatamente che σ è un morfismo

continuo di gruppi, e che $\sigma(\mathbb{R}) = \mathbb{S}^1$. Inoltre $\ker(\sigma) = \mathbb{Z}$ e, pensando $\mathbb{R}/\mathbb{Z}$ dotato della topologia quoziente. si ottiene che $\mathbb{R}/\mathbb{Z}$ è isomorfo, come **gruppo topologico**, a $\mathbb{S}^1$. Ci servirà, in particolare, osservare che $\mathbb{R}/\mathbb{Z}$ è compatto. Tutto questo può facilmente essere modificato per ottenere il seguente utile risultato.

Proposizione 1.0.2 *Si consideri il gruppo topologico $\mathbb{R}$ e si scelga $0 \neq a \in \mathbb{R}$. Posto $N = \langle a \rangle$ il sottogruppo generato da a, i gruppi $\mathbb{R}/N$ ed $\mathbb{S}^1$ sono isomorfi come gruppi topologici. In particolare $\mathbb{R}/N$ è compatto.*

Per dimostrarlo si osserva che N è isomorfo a $\mathbb{Z}$ e si modifica il morfismo σ in modo che la sua immagine resti invariata ma il nucleo sia N.

Sia V uno spazio vettoriale su $\mathbb{R}$ di dimensione n. Fissato un isomorfismo $\phi : \mathbb{R}^n \longrightarrow V$, possiamo definire una topologia su V scegliendo come aperti tutti gli insiemi $A \subseteq V$ tali che $\phi^{-1}(A)$ è aperto di $\mathbb{R}^n$. In tal modo ϕ diventa un isomorfismo topologico. Di certo ϕ è continuo per come è stata definita la topologia. Per vedere che ϕ^{-1} è continuo, osserviamo che, se U è un aperto di $\mathbb{R}^n$, $U = \phi^{-1}(\phi(U))$, e quindi $\phi(U) \in \mathcal{A}_\phi$. Questo dice the ϕ^{-1} è continuo. Scelto un altro isomorphismo $\psi : \mathbb{R}^n \longrightarrow V$, possiamo considerare la mappa (tra gruppi topologici)

$$\sigma = \psi\phi^{-1} : (V, \mathcal{A}_\phi) \longrightarrow (V, \mathcal{A}_\psi)$$

Questo è un isomorfismo continuo, perché composizione di isomorfismi continui. Lo stesso vale per σ^{-1}, e quindi σ è un isomorfismo di gruppi topologici. Pertanto $\mathcal{A}_\phi = \mathcal{A}_\psi = \mathcal{A}$, e questa topologia, che dipende quindi solo dalla topolgia di $\mathbb{R}^n$, sarà quella di cui doteremo ogni $\mathbb{R}$-spazio vettoriale. Quindi, quando dovremo considerare uno spazio vettoriale reale V di dimensione n, potremo supporre, se necessario, che V sia $\mathbb{R}^n$. Inoltre quello che abbiamo appena visto ci dice che, scelte una base $x_1, \ldots, x_n$ di $\mathbb{R}^n$ e $v_1 \ldots, v_n$ di V, l'unica funzione lineare tale che $\sigma(x_i) = v_i$ per ogni i, è un isomorfismo topologico. Quindi ogni isomorfismo lineare tra V ed $\mathbb{R}^n$ è un isomorfismo topologico. Sia ϕ uno di questi isomorfismi e si consideri l'insieme

$$\mathcal{B}_\phi = \{\phi(B) \mid B \subseteq \mathbb{R}^n \text{ è limitato}\}.$$

Si controlla facilmente che tale insieme non dipende da ϕ. I suoi elementi sono i *sottoinsiemi limitati* d V.

Capitolo 2

Reticoli

Diamo ora la definizione di un tipo di struttura di cui faremo grande uso in seguito.

Definizione 2.0.1 *Sia V un $\mathbb{R}$-spazio vettoriale di dimensione finita. Un* reticolo *in V è un sottogruppo generato da una base di V.*

Se V ha dimensione n e $v_1, \ldots, v_n$ è una base, il reticolo associato a tale base è

$$\langle v_1, \ldots, v_n \rangle = \Big\{ \sum_{i=1}^{n} a_i v_i \mid a_i \in \mathbb{Z} \, \forall i \Big\}.$$

Dato che gli elementi di una base sono indipendenti su $\mathbb{R}$, a maggior ragione lo sono su $\mathbb{Z}$. Allora un reticolo in V è un gruppo libero di rango n, quindi isomorfo a $\mathbb{Z}^n$.

Diamo ora una caratterizzazione dei reticoli. Gli spazi vettoriali su $\mathbb{R}$ si intenderanno dotati della topologia discussa in precedenza. Se X è un sottoinsieme dello spazio vettoriale reale V, indichiamo con $\langle X \rangle_{\mathbb{R}}$ il sottospazio vettoriale generato da X. Il simbolo $\langle X \rangle_{\mathbb{Z}}$ indicherà invece il sottogruppo generato da X.

Teorema 2.0.2 *Siano V uno spazio vettoriale su $\mathbb{R}$ di dimensione n ed A un sottogruppo di V. Sono equivalenti:*

1. *A è un reticolo in V.*
2. *A è discreto e V/A è compatto.*
3. *$\langle A \rangle_{\mathbb{R}} = V$ e, per ogni sottoinsieme $B \subseteq V$ limitato, l'insieme $B \cap A$ è finito.*

Dimostrazione Senza perdere di generalità possiamo pensare $V = \mathbb{R}^n$. Indicheremo con $e_1, e_2, \ldots, e_n$ gli elementi della base canonica.

1) $\Longrightarrow$ 2).

Il reticolo A sia generato dalla base $v_1, v_2, \ldots, v_n$. Allora, detta σ l'unica funzione lineare che soddisfa $\sigma(v_i) = e_i$ per ogni $i = 1, \ldots, n$, abbiamo che σ è un isomorfismo topologico e $\sigma(A) = E = \langle e_1, \ldots e_n \rangle_{\mathbb{Z}}$ è un reticolo. Chiaramente E è discreto e quindi anche A è discreto. Osserviamo ora che $V \simeq \oplus_{i=1}^n \langle v_i \rangle_{\mathbb{R}}$ mentre $A \simeq \oplus_{i=1}^n \langle v_i \rangle_{\mathbb{Z}}$. Pertanto si ottiene

$$V/A \simeq \frac{\oplus_{i=1}^n \langle v_i \rangle_{\mathbb{R}}}{\oplus_{i=1}^n \langle v_i \rangle_{\mathbb{Z}}} \simeq \bigoplus_{i=1}^n \frac{\langle v_i \rangle_{\mathbb{R}}}{\langle v_i \rangle_{\mathbb{Z}}}.$$

Dato che ogni quoziente $\langle v_i \rangle_{\mathbb{R}} / \langle v_i \rangle_{\mathbb{Z}}$ è isomorfo ad $\mathbb{R}/\mathbb{Z}$, usando l'esempio precedente abbiamo che V/A è isomorfo, come gruppo topologico, a $(\mathbb{S}^1)^n$ ed è pertanto compatto.

2) $\Longrightarrow$ 3).

Poniamo $W = \langle A \rangle_{\mathbb{R}}$. Se $W \neq V$ allora V/W è isomorfo ad $\mathbb{R}^k$ dove $k = \dim(V) - \dim(W) \geq 1$. Dato che A è sottogruppo di W, il terzo teorema di isomorfismo per gruppi topologici ci dice che V/W è isomorfo al quoziente $(V/A)/(W/A)$ ed è quindi immagine, tramite un morfismo continuo, di V/A. Dato che ogni immagine continua di un compatto è compatta, abbiamo una contraddizione. Ne segue che $W = V$.

Sia ora B un sottoinsieme limitato e supponiamo che $A \cap B$ sia infinito. Dato che anche la chiusura di B è un insieme limitato, possiamo supporre che B sia chiuso, quindi compatto. Dato che $A \cap B$ è un sottoinsieme numerabile di un compatto, contiene una successione infinita $\{x_i \mid i \in \mathbb{N}\}$ che converge ad un certo $x \in B$. In particolare la successione è di Cauchy e, a meno di passare ad una sottosuccessione, possiamo supporre che $0 < |x_i - x_{i-1}| < 2^{-i}$ per ogni $i \geq 1$ (qui $|\cdot|$ indica l'usuale norma di $\mathbb{R}^n$). Ciascuno degli elementi $y_i = x_i - x_{i-1}$ appartiene ad A e chiaramente $\lim y_i = 0 \in A$. Questo vuol dire che 0 non è un punto isolato di A, contraddicendo il fatto che A è discreto.

3) $\Longrightarrow$ 1).

Dato che $\langle A \rangle_{\mathbb{R}} = V$, A deve contenere una base di V. Sia $v_1, v_2, \ldots, v_n$ una tale base e poniamo $M = \langle v_1, \ldots, v_n \rangle_{\mathbb{Z}}$. Chiaramente $M \leq A$. Prendiamo ora un generico elemento $a \in A$. Usando il fatto che i v_i formano una base di V, possiamo scrivere $a = \sum_{i=1}^n \alpha_i v_i$ con gli α_i numeri reali. Ogni α_i si scrive come $\alpha_i = m_i + \lambda_i$ dove $m_i = \lfloor \alpha_i \rfloor$ (la parte intera di α_i) e $\lambda_i = \alpha_i - m_i$ (la parte frazionaria di α_i). Gli m_i sono interi mentre ciascun λ_i appartiene all'intervallo $[0, 1)$. Abbiamo quindi

$$a = \sum_{i=1}^n \alpha_i v_i = \sum_{i=1}^n m_i v_i + \sum_{i=1}^n \lambda_i v_i.$$

L'elemento $m_a = \sum_{i=1}^n m_i v_i$ appartiene ad M (e quindi ad A), mentre $b_a = \sum_{i=1}^n \lambda_i v_i$ è nell'insieme $B = \sum_{i=1}^n [0.1) v_i$, che è un insieme limitato. Dato che $b_a = a - m_a$, anche b_a appartiene ad A, e quindi $b_a \in A \cap B$. Ne deduciamo che $A = M + \langle A \cap B \rangle_{\mathbb{Z}}$. Per ipotesi $A \cap B$ è finito e allora A è un gruppo finitamente generato. Per questo motivo A è isomorfo ad un gruppo del tipo $\mathbb{Z}^m \oplus F$ con F finito ma, essendo A un sottogruppo di $\mathbb{R}^n$, non ha elementi di

periodo finito. Quindi A è libero e indichiamo con m il suo rango. Il sottogruppo M è libero di rango n ed il quoziente A/M può essere descritto, per quanto visto in precedenza, come

$$A/M = \{b + M \mid b \in A \cap B\}.$$

Di conseguenza A/M è finito. Sappiamo che questo accade solo quando M ha lo stesso rango di A, quindi $m = n$ ed un qualsiasi sistema libero $\mathcal{L}$ di generatori di A deve essere una base di V, visto che $\langle A\rangle_{\mathbb{R}} = \langle \mathcal{L}\rangle_{\mathbb{R}}$. Quindi A è un reticolo. □

Definizione 2.0.3 *Dati A, un reticolo in $\mathbb{R}^n$, ed una sua base $\mathbf{v} = \{v_1, v_2, \ldots, v_n\}$, l'insieme $D = \{\sum_{i=1}^n \lambda_i v_i \mid \lambda_i \in [0,1)\ \forall i\} = \sum_{i=1}^n [0,1)v_i$ si dice un* dominio fondamentale *di A.*

Un dominio fondamentale dipende dalla base scelta, quindi lo stesso reticolo ammette diversi domini fondamentali. Se $v_1, v_2, \ldots v_n$ è una base di A e D è il corrispondente dominio fondamentale, allora $\mathbb{R}^n = \bigcup_{v\in A}(D + v)$ e, se $(D + v) \cap (D + w) \neq \emptyset$, deve essere $v = w$. Infatti, se $(D+v)\cap(D+w) \neq \emptyset$, un elemento nell'intersezione è dellla forma $d_1+v = d_2+w$ per opportuni $d_1, d_2 \in D$. Allora $v - w = d_1 - d_2$ e, scrivendo tutti i vettori rispetto alla base $v_1, v_2, \ldots v_n$, si vede che $v - w$ è combinazione intera degli elementi della base, mentre i coefficienti nella scrittura di $d_1 - d_2$ sono tutti numeri reali in modulo strettamente minori di 1. L'unica possibilità è quindi che siano tutti nulli, e di conseguenza $v = w$.

L'insieme $\mathbb{R}^n$ è anche dotato di una misura μ, quella di Lebesgue. Possiamo allora calcolare il volume del dominio fondamentale D che di certo è un insieme misurabile. Se scegliamo un'altra base $\mathbf{w} = \{w_1, \ldots, w_n\}$ per A, ed $M \in M(n, \mathbb{Z})$ è la matrice di passaggio tra le due basi (ovvero $\mathbf{w} = M\mathbf{v}$), abbiamo che, detto $\overline{D}$ il dominio fondamentale rispetto alla nuova base, $\mu(\overline{D}) = |\det(M)|\,\mu(D)$. Dato che M è la matrice di passaggio tra due basi di A, il suo determinante è ± 1. Possiamo allora dare la seguente definizione.

Definizione 2.0.4 *Siano A un reticolo in $\mathbb{R}^n$ e D un suo dominio fondamentale. Definiamo il* covolume *di A come* $\mathrm{cov}(A) = \mu(D)$.

Scelta una base $v_1, \ldots, v_n$ per il reticolo A, il covolume è il valore assoluto del determinante della matrice $K = (v_1 v_2 \cdots v_n)$, ovvero la matrice le cui colonne sono le coordinate, rispetto alla base canonica, dei vettori della base.

Capitolo 3

Teorema di Minkowski

In questa sezione dimostreremo un importante teorema che, pur nella sua semplicità, ha diverse conseguenze di notevole importanza. Iniziamo con un lemma.

Lemma 3.0.1 *Siano X un sottoinsieme di $\mathbb{R}^n$ limitato e misurabile ed L un reticolo in $\mathbb{R}^n$. Si consideri inoltre $\pi : \mathbb{R}^n \longrightarrow \mathbb{R}^n/L$ la proiezione canonica. Se $\mathrm{cov}(L) < \mu(X)$, allora la restrizione di π ad X non è iniettiva.*

Dimostrazione Scegliamo un dominio fondamentale D per L e, per ogni $v \in L$, poniamo $X_v = X \cap (D + v)$. Definiamo poi $Y_v = X_v - v$. Osserviamo che

- gli insiemi X_v sono non vuoti solo per un numero finito di v, dato che X è limitato. Poniamo $I = \{v \mid X_v \neq \emptyset\}$;
- se $v \neq w$ allora $X_v \cap X_w = \emptyset$, visto che $(D + v) \cap (D + w) = \emptyset$;
- $\mu(X_v) = \mu(Y_v)$ dato che la misura di Legesgue è invariante per traslazioni;
- $Y_v \subseteq D$ per ogni $v \in L$.

Abbiamo quindi $\mu(X) = \sum_{v\in I} \mu(X_v) = \sum_{v\in I} \mu(Y_v)$. Ne deduciamo che, per almeno una coppia v, w di elementi distinti di I, deve essere $Y_v \cap Y_w \neq \emptyset$. Per convincerci di questo basta osservare che, se gli insiemi Y_v fossero tutti disgiunti, avremmo $\mu(\bigcup_{v\in I} Y_v) = \sum_{v\in I} \mu(Y_v)$ e, dato che $\bigcup_{v\in I} Y_v \subseteq D$, si otterebbe

$$\mathrm{cov}(L) = \mu(D) \geq \mu(\bigcup_{v\in I} Y_v) = \sum_{v\in I} \mu(Y_v) = \sum_{v\in I} \mu(X_v) = \mu(\bigcup_{v\in I} X_v) = \mu(X) > \mathrm{cov}(L)$$

una contraddizione. Scelti $v, w \in I$ in modo opportuno, abbiamo $Y_v \cap Y_w \neq \emptyset$ e possiamo allora trovare $x_1, x_2 \in X$ tali che $x_1 - v = x_2 - w \in Y_v \cap Y_w$. Da questo si ricava $x_2 = x_1 + (w - v)$ e, dato che $w - v \in L$, si ha $\pi(x_2) = x_1 + (w - v) = x_1 + (w - v) + L = x_1 + L = \pi(x_1)$. Quindi la restrizione di π ad X non è iniettiva, visto che $x_2 - x_1 = w - v \neq 0$. □

Se X è un sottoinsieme di $\mathbb{R}^n$, diciamo che è *simmetrico* se, ogni volta che $x \in X$, allora anche $-x \in X$. Ricordiamo infine che è possibile provare che ogni sottoinsieme di $\mathbb{R}^n$ che sia convesso e limitato, è misurabile secondo Lebesgue. Possiamo ora enunciare e dimostrare il *Teorema del corpo convesso di Minkowski.*

Teorema 3.0.2 *Siano X un sottoinsieme convesso, limitato e simmetrico di $\mathbb{R}^n$ ed L un reticolo di $\mathbb{R}^n$. Se $2^n \mathrm{cov}(L) < \mu(X)$ allora l'insieme $L \cap X$ contiene almeno un elemento diverso da 0.*

Dimostrazione Il reticolo $2L$ ha covolume $2^n \mathrm{cov}(L)$ e quindi, per il lemma 3.0.1, esistono $x, y \in X$ distinti ma tali che $x + 2L = y + 2L$. Dato che $x - y \in 2L$ si ha $0 \neq z = \frac{1}{2}(x - y) \in L$. L'insieme X è simmetrico, quindi $-y \in X$. L'elemento z si scrive come

$$z = \frac{1}{2}x + \frac{1}{2}(-y)$$

ed è pertanto una combinazione convessa di due punti di X. Essendo X convesso abbiamo $z \in X$ ed il teorema è dimostrato. □

Per dare un esempio della utilità di questo risultato, lo usiamo per dimostrare il *Teorema dei quattro quadrati* di Lagrange. Avremo bisogno di un fatto, la cui dimostrazione è lasciata per esercizio.

Lemma 3.0.3 *Sia $\mathbb{F}$ un campo finito. Allora ogni elemento di $\mathbb{F}$ è somma di due quadrati.*

Teorema 3.0.4 *Ogni numero naturale è somma di quattro quadrati.*

Dimostrazione Per prima cosa mostriamo che è sufficiente provare il teorema per i numeri primi. Per vederlo dobbiamo ricordare alcuni fatti elementari sui quaternioni. Se $q = a + bi + cj + dk \in \mathbb{H}$ è un quaternione, la sua norma è definita da $N(q) = a^2 + b^2 + c^2 + d^2$ e per ogni $u, v \in \mathbb{H}$ vale $N(uv) = N(u)N(v)$. Usando questo si vede immediatamente che, se a, b, c, d e x, y, z, w, sono numeri naturali, allora $(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + w^2)$ è ancora la somma di quattro quadrati di numeri naturali. Questa osservazione ci dice che è sufficiente dimostrare che ogni numero primo è somma di quattro quadrati di numeri naturali. La cosa è vera per il primo 2, quindi sia $p \in \mathbb{N}$ un primo dispari. Usando il Lemma 3.0.3 nel caso in cui $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$, possiamo trovare due naturali u, v tali che $u^2 + v^2 + 1 \equiv 0 \pmod{p}$. Definiamo

$$L = \{(x, y, z, w) \in \mathbb{Z}^4 \mid z \equiv ux + vy \pmod{p} \quad \text{e} \quad w \equiv uy - vx \pmod{p}\}.$$

Si controlla immediatamente che L è un sottogruppo di $\mathbb{R}^4$ e, scrivendo esplicitamente le due condizioni date dalle congruenze, si ottiene

$$L = \{(x, y, ux+vy+kp, uy-vx+tp) \mid x, y, k, t \in \mathbb{Z}\} = \langle (1, 0, u, -v), (0, 1, v, u), (0, 0, p, 0), (0, 0, 0, p) \rangle_{\mathbb{Z}}.$$

Il gruppo L è quindi un reticolo ed il suo covolume è dato da

$$\mathrm{cov}(L) = \left| \det \begin{pmatrix} 1 & 0 & u & -v \\ 0 & 1 & v & u \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{pmatrix} \right| = p^2.$$

Detta $B(r)$ la palla di $\mathbb{R}^4$ di centro 0 e raggio r, abbiamo che $\mu(B(r)) = \pi^2 r^4/2$. Scegliamo r in modo che $r^2 = 1.9p$. Con questa scelta si ha $r^4 > 32p^2/\pi^2$ e quindi

$$2^4 \mathrm{cov}(L) = 2^4 p^2 < \pi^2 r^4/2 = \mu(B(r))$$

per cui è possibile applicare il teorema 3.0.2. Prendiamo quindi $0 \neq x = (a, b, c, d) \in L \cap B(r)$. Dato che x appartiene a $B(r)$ la sua norma non supera r^2. Pertanto $|x| = a^2 + b^2 + c^2 + d^2 \leq r^2 < 2p$. Il vettore x è anche un elemento di L, quindi $c \equiv ua + vb \pmod{p}$ e $d \equiv ua - vb \pmod{p}$. Allora

$$a^2 + b^2 + c^2 + d^2 \equiv a^2 + b^2 + (ua + vb)^2 + (ua - vb)^2 \pmod{p}.$$

Ma $(ua + vb)^2 + (ua - vb)^2 = a^2(u^2 + v^2) + b^2(u^2 + v^2)$ e quindi

$$a^2+b^2+c^2+d^2 \equiv a^2+b^2+a^2(u^2+v^2)+b^2(u^2+v^2) = a^2(u^2+v^2+1)+b^2(u^2+v^2+1) \equiv 0 \pmod{p}.$$

Abbiamo allora che $0 < a^2 + b^2 + c^2 + d^2 < 2p$ e p divide $a^2 + b^2 + c^2 + d^2$. L'unica possibilità è che valga $p = a^2 + b^2 + c^2 + d^2$, ed il teorema è dimostrato. □

Capitolo 4

Lo spazio $V_{\mathbb{F}}$

Sia $\mathbb{F}$ un campo di numeri di grado n e si scelga una sua immersione σ. Diremo che σ è *reale* se $\sigma(\mathbb{F}) \leq \mathbb{R}$, altrimenti σ sarà detta *complessa*. Se σ è un'immersione complessa, anche la sua coniugata $\overline{\sigma}$ è un'immersione complessa ed è distinta da σ. Questo ci dice che le immersioni complesse sono sempre in numero pari. Se indichiamo con s il numero di immersioni reali di $\mathbb{F}$, e con $2t$ il numero di immersioni complesse, abbiamo $n = s + 2t$. Il numero t indica il numero di immersioni complesse *a meno di coniugio*. Ad esempio

- se $\mathbb{F} = \mathbb{Q}[\sqrt{d}]$ con $d > 0$ intero libero da quadrati, allora $s = 2, t = 0$;
- se $\mathbb{F} = \mathbb{Q}[\sqrt{d}]$ con $d < 0$ intero libero da quadrati, allora $s = 0, t = 1$;
- se $\mathbb{F} = \mathbb{Q}[\omega]$ con ω radice m-esima primitiva di 1, allora $s = 0$ e $t = \varphi(m)/2$.

D'ora in avanti, fissato un campo di numeri di grado n, scrivendo $n = s + 2t$ intenderemo che gli interi s, t sono quelli appena definiti, ovvero il numero di immersioni reali e il numero di immersioni complesse a meno di coniugio. Definiamo lo spazio vettoriale reale

$$V_{\mathbb{F}} = (\oplus_{i=1}^{s} \mathbb{R}) \oplus (\oplus_{i=1}^{t} \mathbb{C}) = \mathbb{R}^s \oplus \mathbb{C}^t.$$

Questo spazio ha dimensione $s + 2t = n$, in quanto ogni addendo del tipo $\mathbb{C}$ è un $\mathbb{R}$-spazio di dimensione 2.

Siano ora $\sigma_1, \sigma_2, \ldots, \sigma_s$ le immersioni reali di $\mathbb{F}$ e, dopo aver selezionato un elemento per ciascuna coppia di immersioni complesse coniugate, indichiamo tali elementi con $\sigma_{s+1}, \sigma_{s+2}, \ldots, \sigma_{s+t}$ (quindi σ_{s+i} e σ_{s+j} non sono mai coniugate se $i \neq j$). Una volta fatta questa scelta abbiamo una funzione $\sigma : \mathbb{F} \longrightarrow V_{\mathbb{F}}$ definita da

$$\sigma(x) = (\sigma_1(x), \sigma_2(x), \ldots, \sigma_s(x), \sigma_{s+1}(x), \ldots, \sigma_{s+t}(x)).$$

La funzione σ dipende dalla scelta delle immersioni complesse. Quando, fissato un campo di numeri $\mathbb{F}$, parleremo di σ, daremo per scontato che tale scelta sia stata effettuata.

La funzione σ è $\mathbb{Q}$-lineare e possiede la seguente importante proprietà

Proposizione 4.0.1 *Se $\mathbb{F}$ è un campo di numeri di grado n e $\{v_1, \dots, v_n\}$ è una $\mathbb{Q}$-base di $\mathbb{F}$, allora $\{\sigma(v_1), \dots, \sigma(v_n)\}$ è una $\mathbb{R}$-base di $V_{\mathbb{F}}$.*

Dimostrazione Iniziamo enumerando le immersioni nel modo consueto $\sigma_1, \dots, \sigma_s, \sigma_{s+1}, \dots, \sigma_{s+t}$ e ponendo

$$\sigma_l(v_k) = \begin{cases} x_{lk} & \text{se } 1 \leq l \leq s \\ y_{lk} + iz_{lk} & \text{se } s+1 \leq l \leq s+t \end{cases}$$

Consideriamo la matrice M la cui k-esima riga è il vettore $\sigma(v_k) = (\sigma_1(v_k), \dots, \sigma_{s+t}(v_k))$. Per dimostre il nostro risultato dovremo provare che le righe di M sono indipendenti su $\mathbb{R}$. La matrice M ha n-righe ed $s+t$ colonne. Le ultime t colonne contengono però numeri complessi e possiamo, pertanto, pensarle come due colonne di numeri reali nel senso che, se W è una di tali colonne, la scriviamo come $W = Y + iZ$, con Y, Z vettori reali, e la sostituiamo con la coppia (YZ). Una volta compiuta tale operazione con tutte le colonne complesse, possiamo vedere M come una matrice $n \times n$ a coefficienti reali. Volendo essere espliciti scriviamo

$$M = (X_1 X_2 \cdots X_s Y_{s+1} Z_{s+1} \cdots Y_{s+t} Z_{s+t})$$

dove

$$X_l = \begin{pmatrix} x_{l1} \\ x_{l2} \\ \vdots \\ x_{ln} \end{pmatrix} = \begin{pmatrix} \sigma_l(v_1) \\ \sigma_l(v_2) \\ \vdots \\ \sigma_l(v_n) \end{pmatrix} \quad Y_l = \begin{pmatrix} y_{l1} \\ y_{l2} \\ \vdots \\ y_{ln} \end{pmatrix} \quad \text{e } Z_l = \begin{pmatrix} z_{l1} \\ z_{l2} \\ \vdots \\ z_{ln} \end{pmatrix}$$

Dato che ora M è vista come matrice $n \times n$ possiamo vedere che le sue righe sono indipendenti mostrando che $\det(M) \neq 0$. A questo scopo è conveniente pensare la matrice M a coefficienti in $\mathbb{C}$. Eseguiremo alcune operazioni sulle colonne di M, allo scopo di ottenere una matrice il cui determinante è più semplice da calcolare. Iniziamo prendendo in considerazione la sottomatrice $(Y_l Z_l)$. Al posto di questa sottomatrice inseriamo in M la sottomatrice $(Y_l + iZ_l \, Y_l - iZ_l)$. Se chiamiamo M_1 questa nuova matrice vediamo, usando il fatto che il determinante è una funzione multilineare delle colonne, che vale la relazione $\det(M_1) = (-2i)\det(M)$. Infatti, sostituendo alla colonna Y_l la colonna $Y_l + iZ_l$ il determinante non cambia. Ma, per ottenere la colonna $Y_l - iZ_l$, dobbiamo moltiplicare Z_l per $-2i$ (ed il determinante viene moltiplicato per $-2i$) e quindi aggiungere la colonna $Y_l - iZ_l$ (e questo non cambia il valore del determinante). È importante osservare che

$$Y_l + iZ_l = \begin{pmatrix} \sigma_l(v_1) \\ \sigma_l(v_2) \\ \vdots \\ \sigma_l(v_n) \end{pmatrix} \quad Y_l - iZ_l = \begin{pmatrix} \overline{\sigma_l}(v_1) \\ \overline{\sigma_l}(v_2) \\ \vdots \\ \overline{\sigma_l}(v_n) \end{pmatrix}$$

Una volta eseguito questo processo per ciascuna sottomatrice $(Y_l Z_l)$, otteniamo una nuova matrice M_0 e abbiamo $\det(M_0) = (-2i)^t \det(M)$. Allora $\det(M) \neq 0$ se e solo se $\det(M_0) \neq 0$.

Dato che l'insieme delle immersioni di $\mathbb{F}$ è $\{\sigma_i, \sigma_{s+j}, \overline{\sigma_{s+j}} \mid i = 1, \dots, s \quad j = 1, \dots, t\}$, vediamo che, se rinominiamo opportunamente le immersioni come $\{\tau_1, \tau_2, \dots, \tau_n\}$, la matrice M_0 ha, nella posizione ij, l'elemento $\tau_j(v_i)$. Allora $(\det(M_0))^2 = \Delta[v_1, v_2, \dots, v_n]$, e questo è diverso da 0 perché $\{v_1, v_2 \dots, v_n\}$ è una base di $\mathbb{F}$. Quindi anche $\det(M) \neq 0$ e la tesi è dimostrata. □

Se analizziamo con attenzione la dimostrazione della proposizione 4.0.1, possiamo ricavare un corollario di grande utilità in diverse situazioni. Gli interi s, t hanno l'usuale significato.

Corollario 4.0.2 *Siano $\mathbb{F}$ un campo di numeri di grado $n = s + 2t$, I un ideale non nullo di $\mathcal{O}_\mathbb{F}$ e σ l'immersione di $\mathbb{F}$ in $V_\mathbb{F}$. Allora $\sigma(I)$ è un reticolo in $V_\mathbb{F}$ e*

$$\mathrm{cov}(\sigma(I)) = \frac{1}{2^t} N(I) \sqrt{|\Delta_\mathbb{F}|}.$$

Dimostrazione Sia $\{v_1, v_2 \dots v_n\}$ una base del gruppo additivo di $\mathcal{O}_\mathbb{F}$. L'ideale I, pensato come gruppo additivo, è anche lui libero di rango n, generato da una base $\{w_1, \dots, w_n\}$. Ricordiamo che $\Delta_\mathbb{F} = \Delta[v_1, v_2 \dots v_n]$ e $|\Delta[w_1, \dots, w_n]| = N(I)^2 |\Delta_\mathbb{F}|$. Dato che $\{w_1, \dots, w_n\}$ è un insieme indipendente, è anche una $\mathbb{Q}$-base di $\mathbb{F}$. La proposizione 4.0.1 ci dice che $\{\sigma(w_1), \dots, \sigma(w_n)\}$ è una base di $V_\mathbb{F}$ per cui $\sigma(I) = \sigma(\langle w_1, \dots, w_n \rangle_\mathbb{Z}) = \langle \sigma(w_1), \dots, \sigma(w_n) \rangle_\mathbb{Z}$ è un reticolo in $V_\mathbb{F}$. Dato che

$$\mathrm{cov}(L) = \left| \det \begin{pmatrix} \sigma(w_1) \\ \sigma(w_2) \\ \vdots \\ \sigma(w_n) \end{pmatrix} \right|$$

la dimostrazione precedente dice che

$$\mathrm{cov}(L) = \frac{1}{2^t} \sqrt{|\Delta[w_1, \dots, w_n]|} = \frac{1}{2^t} N(I) \sqrt{|\Delta_\mathbb{F}|}$$

come volevamo dimostrare. □

Sia $x = (x_1, \dots, x_{s+t}) \in V_\mathbb{F}$ e scegliamo una sua coordinata x_i. Se $i \leq s$ allora x_i è reale e $|x_i|$ indicherà l'usuale valore assoluto. Altrimenti x_i è complesso e poniamo $\|x_i\| = \sqrt{x\overline{x}}$. Per ogni numero reale c definiamo

$$\Omega(c) = \left\{ x \in V_\mathbb{F} \;\middle|\; \sum_{i=1}^{s} |x_i| + 2 \sum_{i=1}^{t} \|x_{s+i}\| \leq c \right\}.$$

L'insieme $\Omega(c)$ è limitato, simmetrico e convesso ed è importante conoscerne la misura.

Lemma 4.0.3 *Se $n = s + 2t$ e c è un numero reale strettamente positivo, si ha*

$$\mu(\Omega(c)) = 2^s \left(\frac{\pi}{2}\right)^t \frac{c^n}{n!}.$$

Dimostrazione Per induzione su $s + t$.

Se $s + t = 1$ dobbiamo considerare due casi. Quando $s = 1$ e $t = 0$, allora $\Omega(c) = \{ x \in \mathbb{R} \mid |x| \leq c \}$ ed è evidente che la misura di questo insieme è $2c$. Se, invece, $s = 0$ e $t = 1$, abbiamo $\Omega(c) = \{ x \in \mathbb{C} \mid 2\|x\| \leq c \}$. Quindi $\Omega(c)$ è un disco di raggio $c/2$ e la sua misura vale $\pi c^2/4 = (\pi/2)(c^2/2)$.

Veniamo allora al passo induttivo, la cui dimostrazione deve essere divisa in due parti. Dobbiamo provarlo nel caso sia la variabile s a crescere, e nel caso in cui cresca la variabile t.

Caso 1. $s \longmapsto s + 1$.

In questo caso $n = s + 1 + 2t$. Abbiamo

$$\mu(\Omega(c)) = \int_{\Omega(c)} d\mu = \int_{-c}^{c} \mu(\Omega(c - |x_1|) dx_1$$

e, sfruttando l'ipotesi induttiva,

$$\int_{-c}^{c} \mu(\Omega(c - |x_1|)) dx_1 = \int_{-c}^{c} 2^s \Big(\frac{\pi}{2}\Big)^t \frac{(c - |x_1|)^{n-1}}{(n-1)!} dx_1 = 2^s \Big(\frac{\pi}{2}\Big)^t \frac{1}{(n-1)!} \int_{-c}^{c} (c - |x_1|)^{n-1} dx_1$$

da cui la tesi segue immediatamente.

Caso 2. $t \longmapsto t + 1$.

Se indichiamo con z_1 la prima delle componenti complesse e poniamo $n = s + 2(t + 1))$, abbiamo

$$\mu(\Omega(c)) = \int_{\Omega(c)} d\mu = \int_{\|z_1\| \leq c/2} \mu(\Omega(c - 2\|z_1\|) dz_1 = 2^s \Big(\frac{\pi}{2}\Big)^t \frac{1}{(n-2)!} \int_{\|z_1\| \leq c/2} (c - 2\|z_1\|)^{n-2} dz_1$$

dove, per l'ultima uguaglianza, abbiamo usato l'ipotesi induttiva. Possiamo concentraci allora nel calcolo dell'ultimo integrale. Passando alle coordinate polari ρ, θ, si ottiene

$$\int_{\|z_1\| \leq c/2} (c - 2\|z_1\|)^{n-2} dz_1 = \int_0^{2\pi} \int_0^{c/2} (c - 2\rho)^{n-2} \rho d\theta d\rho = 2\pi \int_0^{c/2} (c - 2\rho)^{n-2} \rho d\rho.$$

Ponendo $t = c - 2\rho$ si ottiene facilmente che il valore che stiamo cercando è $\pi c^n/2(n-1)n$. Ne segue che, anche in questo caso, la tesi è vera ed il lemma è dimostrato. □

Useremo la seguente (e ben nota) disguaglianza tra media geometrica e media aritmetica.

Lemma 4.0.4 *Se $a_1, a_2, \ldots, a_N$ sono sumeri reali positivi, allora $(\prod_{i=1}^N a_i)^{1/N} \leq (\sum_{i=1}^N a_i)/N$.*

Il prossimo risultato dice, in sostanza, che ogni ideale non nullo in un anello di numeri contiene elementi diversi da 0 e di norma *piccola*.

Proposizione 4.0.5 *Siano $\mathbb{F}$ un campo di numeri di grado $n = s + 2t$ ed I un ideale non nullo di $\mathcal{O}_{\mathbb{F}}$. Allora esiste $\alpha \in I$ tale che $\alpha \neq 0$ e*

$$|N(\alpha)| \leq \Big(\frac{4}{\pi}\Big)^t \frac{n!}{n^n} N(I) \sqrt{|\Delta_{\mathbb{F}}|}.$$

Dimostrazione Facciamo riferimento alle notazioni introdotte nel Lemma 4.0.3. Per ogni naturale $k > 0$ definiamo il numero reale c_k tramite la relazione

$$\mu(\Omega(c_k)) = 2^n \frac{1}{2^t} N(I)\sqrt{|\Delta_{\mathbb{F}}|} + \frac{1}{k}.$$

La successione formata dai c_k è decrescente, come la successione degli insiemi $\Omega(c_k)$ e, definito c tramite l'uguaglianza

$$2^s \Big(\frac{\pi}{2}\Big)^t \frac{c^n}{n!} = 2^n \frac{1}{2^t} N(I)\sqrt{|\Delta_{\mathbb{F}}|},$$

abbiamo $\Omega(c) = \bigcap_{k=1}^{\infty} \Omega(c_k)$.

L'ntersezione tra $\Omega(c_k)$ ed il reticolo $\sigma(I)$ è finita, essendo $\Omega(c_k)$ limitato, quindi per qualche $\overline{k}$ si deve avere

$$\sigma(I) \cap \Omega(c_{\overline{k}}) = \sigma(I) \cap \Omega(c_k) \quad \text{per ogni } k \geq \overline{k}$$

Dato che, per costruzione, $2^n \mathrm{cov}(\sigma(I)) < \mu(\Omega(c_k))$ per ogni k, il Teorema di Minkowski ci assicura che l'insieme $\sigma(I) \cap \Omega(c_{\overline{k}})$ contiene almeno un elemento diverso da 0. Pertanto

$$\sigma(I) \cap \Omega(c) = \sigma(I) \cap \Big(\bigcap_{k=1}^{\infty} \Omega(c_k)\Big) = \sigma(I) \cap \Big(\bigcap_{k \geq \overline{k}} \Omega(c_k)\Big) = \sigma(I) \cap \Omega(c_{\overline{k}})$$

contiene almeno un elemento diverso da 0, che avrà la forma $\sigma(\alpha)$ per un opportuno $\alpha \in I$. Se elenchiamo le immersioni di $\mathbb{F}$ come $\tau_1, \tau_2, \ldots, \tau_n$ vediamo che $\sum_{i=1}^{n} \|\tau_i(\alpha)\| = \sum_{i=1}^{s} |\sigma_i(\alpha)| + 2\sum_{i=1}^{t} \|\sigma_{s+i}(\alpha)\| \leq c$. Usando il Lemma 4.0.4 troviamo

$$|N(\alpha)| = |\prod_{i=1}^{n} \tau_i(\alpha)| = \prod_{i=1}^{s} |\sigma_i(\alpha)| \cdot \prod_{i=1}^{t} \sigma_{s+i}(\alpha) \cdot \prod_{i=1}^{t} \overline{\sigma_{s+i}(\alpha)} \leq \Big(\frac{\sum_{i=1}^{n} \|\tau_i(\alpha)\|}{n}\Big)^n \leq \frac{c^n}{n^n}.$$

Usando il modo in cui è stato definito c, ricaviamo

$$|N(\alpha)| \leq \Big(\frac{4}{\pi}\Big)^t \frac{n!}{n^n} N(I)\sqrt{|\Delta_{\mathbb{F}}|}.$$

La proposizione è quindi dimostrata. □

Prima di dimostrare il teorema principale, ci servono altri due semplici lemmi.

Lemma 4.0.6 *Siano $\mathbb{F}$ un campo di numeri e $\alpha \in \mathcal{O}_{\mathbb{F}}$ un elemento diverso da 0. Se I è l'ideale generato da α allora $N(I) = |N(\alpha)|$.*

Dimostrazione Sia $v_1, v_2, \ldots v_n$ una base per $\mathcal{O}_{\mathbb{F}}$ in modo che ogni intero algebrico si scrive come $\sum_{i=1}^{n} a_i v_i$ con $a_i \in \mathbb{Z}$ per ogni i . Un generico elemento di I ha la forma $\alpha(\sum_{i=1}^{n} a_i v_i) = \sum_{i=1}^{n} a_i(\alpha v_i)$ e pertanto $I = \{ \sum_{i=1}^{n} a_i(\alpha v_i) \mid a_i \in \mathbb{Z} \forall\, i \}$. In altri termini l'ideale I, pensato come gruppo abeliano, è generato dall'insieme $\{\alpha v_1, \alpha v_2, \ldots, \alpha v_n\}$ e quindi vale $|\Delta[\alpha v_1, \ldots, \alpha v_n]| = N(I)\sqrt{|\Delta_{\mathbb{F}}|}$. Se indichiamo con $\sigma_1, \sigma_2, \ldots \sigma_n$ le immersioni di $\mathbb{F}$ abbiamo le seguente relazione

$$M = \begin{pmatrix} \sigma_1(\alpha v_1) & \ldots & \sigma_1(\alpha v_n) \\ \sigma_2(\alpha v_1) & \ldots & \sigma_2(\alpha v_n) \\ \ldots\ldots & \ldots\ldots & \ldots\ldots \\ \sigma_n(\alpha v_1) & \ldots & \sigma_n(\alpha v_n) \end{pmatrix} = \begin{pmatrix} \sigma_1(\alpha) & \ldots & 0 \\ 0 & \sigma_2(\alpha) & 0 \\ 0 & \ldots & 0 \\ 0 & \ldots & \sigma_n(\alpha) \end{pmatrix} \begin{pmatrix} \sigma_1(v_1) & \ldots & \sigma_1(v_n) \\ \sigma_2(v_1) & \ldots & \sigma_2(v_n) \\ \ldots\ldots & \ldots\ldots & \ldots\ldots \\ \sigma_n(v_1) & \ldots & \sigma_n(v_n) \end{pmatrix}$$

da cui ricaviamo $\Delta[\alpha v_1, \ldots, \alpha v_n] = (\det(M))^2 = N(\alpha)^2 \Delta_{\mathbb{F}}$. La tesi segue immediatamente. □

Lemma 4.0.7 *Se $\mathbb{F}$ è un campo di numeri ed N un numero reale positivo, gli ideali di $\mathcal{O}_{\mathbb{F}}$ di norma minore di N sono un numero finito.*

Dimostrazione Dato che ogni ideale è prodotto di primi e che la norma è moltiplicativa, è sufficiente provare che $\mathcal{O}_{\mathbb{F}}$ possiede solo un numero finito di ideali primi di norma minore di N. Sia allora n il grado di $\mathbb{F}$ e si scelga $\mathcal{P}$ un ideale primo di norma minore di N. L'ideale $\mathcal{P}$ contiene un unico primo razionale, individuato dalla relazione $\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$, quindi l'ideale $p\mathcal{O}_{\mathbb{F}}$ è contenuto in $\mathcal{P}$. Questo ci dice the $N(\mathcal{P})$ divide $N(p\mathcal{O}_{\mathbb{F}}) = p^n$ e ne segue che $p \leq N$. Pertanto i primi di norma minore di N sono tra quelli che dividono gli ideali del tipo $p\mathcal{O}_{\mathbb{F}}$ con p primo e $p \leq N$. Questi primi sono, ovviamente, in numero finito. □

Possiamo finalmente dimostrare che, per ogni campo di numeri, il gruppo delle classi è finito

Teorema 4.0.8 *Sia $\mathbb{F}$ un campo di numeri. Allora il suo gruppo delle classi è finito.*

Dimostrazione Iniziamo scrivendo il grado di $\mathbb{F}$ come $n = s + 2t$ e ponendo

$$M_{st} = \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}.$$

Questo numero è detto *costante di Minkowski* e dipende solo da $\mathbb{F}$. Se $G = \mathcal{C}l(\mathbb{F})$ è il gruppo delle classi di $\mathbb{F}$ e $\omega \in G$, osserviamo che ω contiene un ideale di $\mathcal{O}_{\mathbb{F}}$. Infatti, preso $J \in \omega$ un qualsiasi ideale frazionario, esiste $0 \neq a \in \mathbb{F}$ tale che $I = aJ \subseteq \mathcal{O}_{\mathbb{F}}$. Quindi I è ideale di $\mathcal{O}_{\mathbb{F}}$ e, indicando con $[\cdot]$ la classe di un ideale in G, abbiamo, $[I] = [J(a)] = [J][(a)] = [J] = \omega$. Il punto centrale della dimostrazione sarà provare che ogni classe $\omega \in G$ contiene un ideale I con $N(I) \leq M_{st}\sqrt{|\Delta_{\mathbb{F}}|}$. A tale scopo prendiamo la classe ω^{-1} e scegliamo un ideale $J \in \omega^{-1}$. Per il Lemma 4.0.5, esiste $0 \neq \alpha \in J$ tale che $|N(\alpha)| \leq M_{st} N(J)\sqrt{|\Delta_{\mathbb{F}}|}$. Dato che $(\alpha) \subseteq J$ abbiamo $J \mid (\alpha)$ e quindi esiste un ideale I tale che $IJ = (\alpha)$. Passando alle classi in G si ottiene $[IJ] = [(\alpha)] = 1$ e quindi $[I][J] = 1$, da cui, ricordando che $[J] = \omega^{-1}$, si vede che $[I] = \omega$. Considerando le norme otteniamo $N((\alpha)) = N(IJ) = N(I)N(J)$ e quindi, usando il Lemma 4.0.6,

$$N(I)N(J) = N((\alpha)) = |N(\alpha)| \leq M_{st} N(J)\sqrt{|\Delta_{\mathbb{F}}|}.$$

Dividendo per $N(J)$ otteniamo $N(I) \leq M_{st}\sqrt{|\Delta_{\mathbb{F}}|}$. Abbiamo cioè provato che, per ogni classe $\omega \in G$, esiste un ideale $I \in \omega$ tale che $N(I) \leq M_{st}\sqrt{|\Delta_{\mathbb{F}}|}$. Allora

$$G = \{\, [I] \mid I \text{ è ideale di } \mathcal{O}_{\mathbb{F}} \,\} = \{\, [I] \mid I \text{ è ideale di } \mathcal{O}_{\mathbb{F}} \text{ e } N(I) \leq M_{st}\sqrt{|\Delta_{\mathbb{F}}|} \,\}.$$

Ma, per il Lemma 4.0.8, solo un numero finito di ideali di $\mathcal{O}_{\mathbb{F}}$ ha norma minore di $M_{st}\sqrt{|\Delta_{\mathbb{F}}|}$ e questo prova che il gruppo G è finito. □.