
UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Corso di Laurea Triennale in Matematica

# Il principio locale-globale e il teorema di Hasse-Minkowski

Relatore:
**Prof. Matteo Longo**

Candidato:
**Paola Mupo**

Matricola:
**1222758**

ANNO ACCADEMICO 2021/2022
23 Settembre 2022

*A mamma, papà*
*e Camilla*

# Indice

# Introduzione

I numeri $p$-adici furono introdotti da Hensel agli inizi del XX secolo come mezzo di utilizzo delle tecniche legate alle serie formali nell'ambito della teoria dei numeri. La loro importanza è cresciuta costantemente ed i numeri $p$-adici si sono rivelati uno strumento essenziale nella teoria dei numeri moderna. L'opera di Hasse e Minkowski sulle forme quadratiche si colloca in questo panorama come uno dei primi e più rilevanti esempi dell'applicazione dei numeri $p$-adici per comprendere più a fondo l'aritmetica dei numeri razionali.
Vediamo brevemente come possono essere presentati i numeri $p$-adici: si veda il Capitolo 1 per maggiori dettagli o altre definizioni equivalenti. È noto che l'insieme $\mathbb{Q}$ dei numeri razionali dotato della distanza euclidea costituisce uno spazio metrico non completo e l'insieme dei reali $\mathbb{R}$ può essere costruito come il suo completamento. Analogamente, per ogni intero primo $p$, definiamo su $\mathbb{Q}$ una distanza diversa da quella usuale, che chiameremo distanza $p$-adica: due numeri $a$ e $b$ sono vicini $p$-adicamente se potenze alte di $p$ dividono la differenza $a - b$. L'insieme dei numeri $p$-adici $\mathbb{Q}_p$ è pertanto definito analiticamente come il completamento di $\mathbb{Q}$ con la distanza $p$-adica e, come sopra accennato, gioca un ruolo primario in teoria dei numeri: *attraverso la luce dei numeri p-adici iniziamo a cogliere le profondità dell'universo matematico così come nel buio della notte distinguiamo meglio gli oggetti celesti* [3]. Su questa scia nel 1920 Hasse scoprì che il lavoro di Minkowski sulle forme quadratiche su $\mathbb{Q}$ poteva essere espresso in termini delle forme quadratiche su $\mathbb{R}$ e $\mathbb{Q}_p$. Questa profonda relazione diede vita al *principio locale-globale* o *principio di Hasse*, un'idea di fondamentale importanza in teoria dei numeri che può sostanzialmente essere tradotta nella seguente affermazione: *una proprietà o un teorema vale su* $\mathbb{Q}$ *se e solo se vale su* $\mathbb{R}$ *e su* $\mathbb{Q}_p$ *per ogni p primo* [2]. Tale principio permette quindi di studiare un problema su $\mathbb{Q}$, come ad esempio trovare le soluzioni razionali di un'equazione razionale, attraverso lo studio dello stesso problema su $\mathbb{R}$ e $\mathbb{Q}_p$. Chiameremo allora $\mathbb{Q}$ il campo *globale* e i suoi completamenti $\mathbb{R}$ e $\mathbb{Q}_p$ campi *locali*.
La tesi si propone di enunciare e dimostrare il teorema che condensa il sopra citato lavoro di Hasse e Minkowski, il quale sancisce la validità del principio locale-globale nel caso degli zeri delle *forme quadratiche*. Una forma quadratica $f$ a coefficienti in un campo $K$ è un polinomio omogeneo di secondo grado del tipo

$$f(X_1, X_2, ..., X_n) = \sum_{i=1}^{n} a_{ii} X_i^2 + 2 \sum_{i<j} a_{ij} X_i X_j \quad \text{dove } a_{ij} \in K$$

Diremo che $f$ rappresenta lo zero su $K$ se l'equazione $f(X_1, X_2, ..., X_n) = 0$ ha una soluzione non banale in $K^n$. Se $K = \mathbb{Q}$, l'immersione del campo dei razionali nei suoi

completamenti $\mathbb{R}$ e $\mathbb{Q}_p$ permette di vedere ogni forma quadratica $f$ a coefficienti in $\mathbb{Q}$ come una forma quadratica su $\mathbb{R}$ e $\mathbb{Q}_p$. Il teorema di Hasse-Minkowski afferma che *una forma quadratica $f$ a coefficienti razionali rappresenta lo zero su $\mathbb{Q}$ se e solo $f$ rappresenta lo zero su $\mathbb{R}$ e $\mathbb{Q}_p$ per ogni primo $p$* [6]. Alla luce di quanto detto fin'ora, una implicazione è triviale: se $f$ ha uno zero razionale ne ha anche uno reale e $p$-adico. L'obbiettivo dell'elaborato è mostrare che tale implicazione è invertibile: l'esistenza di zeri locali ci garantisce l'esistenza di uno zero globale. Il primo capitolo è dedicato alla presentazione dei numeri $p$-adici: giungeremo al cuore della loro definizione analitica, alla quale abbiamo sinteticamente abbozzato, e ne daremo una definizione puramente algebrica, mostrando l'equivalenza tra le due. Tratteremo il problema delle soluzioni di equazioni a valori $p$-adici mostrando come, tramite il *lemma di Hensel*, queste sono costruibili a partire dalle soluzioni delle stesse equazioni ridotte modulo una potenza di $p$, e presenteremo il gruppo moltiplicativo $\mathbb{Q}_p^*$ ed il sottogruppo dei quadrati nel campo dei numeri $p$-adici, $\mathbb{Q}_p^{*2}$. Procederemo poi con una trattazione sulla *legge di reciprocità quadratica*, legata indissolubilmente alle proprietà del *simbolo di Hilbert*, che sarà indispensabile nella caratterizzazione delle forme quadratiche su $\mathbb{Q}_p$. Il terzo capitolo si occupa della presentazione geometrica delle forme quadratiche e ad alcuni importanti risultati di algebra lineare, essenziali per la descrizione delle forme quadratiche su $\mathbb{Q}$ ed i suoi completamenti $\mathbb{R}$ e $\mathbb{Q}_p$. Una volta collezionati tutti gli strumenti necessari e lemmi preliminari, saremo in grado di dimostrare il teorema di Hasse-Minkowski e cogliere a pieno la sua eleganza e profonda portata.
È opportuno precisare che il principio locale-globale non è un asserto universale. Se consideriamo equazioni polinomiali di grado maggiore sul campo dei razionali troviamo numerosi controesempi. Nello specifico, aumentando di grado, il principio locale-globale fallisce per la famiglia delle curve ellittiche definite su $\mathbb{Q}$, cioè delle curve algebriche $E$ di terzo grado non singolari descritte da equazioni del tipo

$$E: \quad Y^2 = f(X) \quad \text{dove } f \text{ è un polinomio di terzo grado su } \mathbb{Q} \text{ privo di radici multiple.}$$

In particolare, detto $E(K)$ l'insieme dei punti della curva sul campo $K$, per $K = \mathbb{Q}, \mathbb{R}$ e $\mathbb{Q}_p$, la corrispondenza tra l'insieme dei punti razionali della curva $E(\mathbb{Q})$ e gli insiemi $E(\mathbb{R})$ e $E(\mathbb{Q}_p)$ per ogni $p$ primo, che vale nel caso delle forme quadratiche, cessa di esistere. Infatti esistono punti $P_p \in E(\mathbb{Q}_p)\ \forall p$ primo e $P_\infty \in E(\mathbb{R})$ tali che $\nexists\ P \in E(\mathbb{Q})$ per cui

$$\begin{array}{ccc} E(\mathbb{Q}) \longrightarrow E(\mathbb{Q}_p) \\ P \longrightarrow P_p \end{array} \quad \text{e} \quad \begin{array}{ccc} E(\mathbb{Q}) \longrightarrow E(\mathbb{R}) \\ P \longrightarrow P_\infty \end{array}$$

Il fatto che il principio locale-globale non valga nel caso delle curve ellittiche deriva (in termini coomologici) da un gruppo congetturalmente finito, il gruppo di Shafarevich-Tate della curva ellittica, che compare nell'enunciato della congettura di Birch e Swinnerton-Dyer, la quale rappresenta una delle questioni irrisolte di maggiore interesse della matematica contemporanea.

# Capitolo 1

# Numeri $p$-adici

In questo capitolo ci occuperemo della definizione analitica e algebrica dei numeri $p$-adici e mostreremo la loro equivalenza.

## 1.1 Definizione analitica

**Definizione 1.1.** *Sia $p$ un numero primo. Ogni numero razionale $a$ può essere scritto come*

$$a = p^m \frac{u}{v}$$

*dove $m$, $u \in \mathbb{Z}$, $v \in \mathbb{Z} \setminus \{0\}$ e $p$ non divide $u$ e $v$. Si definisce la valutazione $p$-adica di $a$ l'intero $m = ord_p(a)$ e per convenzione si pone $ord_p(0) = \infty$.*

**Osservazione 1.1.** *Valgono le seguenti proprietà:*

1. $ord_p(ab) = ord_p(a) + ord_p(b)$
2. $ord_p(a+b) \geq min(ord_p(a), ord_p(b))$
3. *se $ord_p(a) \neq ord_p(b)$ allora $ord_p(a+b) = min(ord_p(a), ord_p(b))$*

Risulta naturale considerare due numeri razionali $a$ e $b$ "vicini" in senso $p$-adico se $ord_p(a-b)$ è molto grande. A tal proposito definiamo una *distanza $p$-adica* su $\mathbb{Q}$:

**Definizione 1.2.** *Sia $a \in \mathbb{Q}$ si definisce il valore assoluto $p$-adico:*

$$|a|_p = p^{-ord_p(a)}$$

*se $a \neq 0$. Se $a = 0$ poniamo $|0|_p = 0$. Si definisce infine la distanza $p$-adica $d_p(a,b)$ come*

$$d_p(a,b) = |a-b|_p$$

**Osservazione 1.2.** $|-|_p$ *soddisfa le seguenti proprietà:*

1. $|ab|_p = |a|_p |b|_p$
2. $|a+b|_p \leq max(|a|_p, |b|_p)$

Si noti che $\mathbb{Q}$ è uno spazio metrico con la distanza $p$-adica $d_p$. In particolare una successione $(x_n)_{n\in\mathbb{N}}$ converge "in senso $p$-adico" ad $a$ se e solo se $d_p(x_n, a) \to 0$ per $n \to \infty$ dunque $ord_p(x_n - a) \to \infty$, ovvero potenze "grandi" di $p$ dividono la differenza $x_n - a$.

**Definizione 1.3.** *$\mathbb{Q}_p$ è il completamento dello spazio metrico $(\mathbb{Q}, d_p)$.*

Più precisamente, sia $S_p$ l'insieme delle successioni in $\mathbb{Q}$ di Cauchy per $d_p$, ovvero delle successioni in $\mathbb{Q}$, $(x_n)_{n\in\mathbb{N}}$, tali che $\forall\epsilon \geq 0\ \exists N \in \mathbb{N}$ tale che $\forall n, m \geq N$ vale $|x_n - x_m|_p \leq \epsilon$. Si definisce la seguente relazione di equivalenza su $S_p$: $(x_n)_{n\in\mathbb{N}}$ e $(y_n)_{n\in\mathbb{N}}$ sono equivalenti se $\forall\epsilon \geq 0\ \exists N \in \mathbb{N}$ tale che $\forall n \geq N$ si ha $|x_n - y_n|_p \leq \epsilon$, ovvero $\lim_n |x_n - y_n|_p \to 0$ per $n \to \infty$. Definisco quindi $\mathbb{Q}_p$ come lo spazio quoziente di $S_p$.
Ogni numero razionale $a$ si identifica con la successione costante uguale ad $a$ dunque $\mathbb{Q}$ si immerge in $\mathbb{Q}_p$. Possiamo ora estendere la valutazione $p$-adica e la distanza $d_p$ a $\mathbb{Q}_p$.

Sia $a \neq 0$ e scegliamo un rappresentante $(x_n)_{n\in\mathbb{N}}$ di $a$. Allora per $n$ grande $ord_p(x_n)$ sarà costante. Infatti, se $a \neq 0$, $(x_n)_{n\in\mathbb{N}}$ non è equivalente alla successione costante uguale a zero, quindi, esiste un $\epsilon \geq 0$ tale che per ogni $N$ esiste un $x_{n_N}$ tale che $n_N \geq N$ e $d_p(x_{n_N}, 0) \geq \epsilon$, cioè $|x_{n_N}|_p \geq \epsilon$. Allora sia $M$ tale che $\epsilon \geq p^{-M}$ e $ord_p(x_{n_N}) \leq M$. So che $(x_n)_{n\in\mathbb{N}}$ è di Cauchy: prendiamo $N$ grande abbastanza tale che, se $n, m \geq N$, $|x_n - x_m|_p < p^{-M}$ cioè $ord_p(x_n - x_m) > M$. Segue che $|x_{n_N} - x_m|_p < p^{-M}$, cioè $ord_p(x_m - x_{n_N}) > M$. Dunque $ord_p(x_{n_N}) \leq M < ord_p(x_m - x_{n_N})$. Segue che

$$ord_p(x_m) = min\,(ord_p(x_{n_N}), ord_p(x_m - x_{n_N})) = ord_p(x_{n_N})$$

per ogni $m \geq N$.

**Definizione 1.4.** *Sia $a \in \mathbb{Q}_p$ si definisce $ord_p(a) = 0$ se $a = 0$. Altrimenti $ord_p(a) = ord_p(x_n)$ per $n$ grande. Si pone inoltre $|a|_p = p^{-ord_p(a)} = \lim_n |x_n|_p$.*

Si noti che $|a|_p$ non dipende dal rappresentante scelto: se $x = [(x_n)_{n\in\mathbb{N}}] = [(y_n)_{n\in\mathbb{N}}]$ allora

$$|x_n|_p \leq |x_n - y_n|_p + |y_n|_p$$

e per $n \to \infty$ ho $\lim_n |x_n|_p \leq \lim_n |y_n|_p$. Analogamente

$$|y_n|_p \leq |y_n - x_n|_p + |x_n|_p$$

da cui $\lim_n |y_n|_p \leq \lim_n |x_n|_p$.

**Proposizione 1.1.** *$\mathbb{Q}_p$ è un campo con le operazioni di somma e prodotto definite naturalmente sulle classi.*

*Dimostrazione.* Siano $x = [(x_n)_{n\in\mathbb{N}}]$ e $y = [(y_n)_{n\in\mathbb{N}}]$, si pone:

$$x + y = [(x_n)_{n\in\mathbb{N}}] + [(y_n)_{n\in\mathbb{N}}] = [(x_n + y_n)_{n\in\mathbb{N}}] \quad xy = [(x_n)_{n\in\mathbb{N}}][(y_n)_{n\in\mathbb{N}}] = [(x_n y_n)_{n\in\mathbb{N}}].$$

Mostriamo che sono delle buone definizioni. Sia $(x'_n)_{n\in\mathbb{N}}$ un altro rappresentante per $x$ e $(y'_n)_{n\in\mathbb{N}}$ un altro rappresentante per $y$. Allora

$$\begin{aligned}\left|x'_n y'_n - x_n y_n\right|_p &= \left|x'_n y'_n - x'_n y_n + x'_n y_n - x_n y_n\right|_p \\ &\leq \max\left(\left|x'_n\right|_p \left|y'_n - y_n\right|_p, |y_n|_p \left|x'_n - x_n\right|_p\right) \to 0\end{aligned}$$

per $n \to \infty$ poiché $|x'_n|_p = |x|_p$ e $|y_n|_p = |y|_p$ per $n$ grande e $x = [(x_n)_{n\in\mathbb{N}}] = [(x'_n)_{n\in\mathbb{N}}]$, $y = [(y_n)_{n\in\mathbb{N}}] = [(y'_n)_{n\in\mathbb{N}}]$. Analogamente:

$$\left|(x'_n + y'_n) - (x_n + y_n)\right|_p \leq max\left(\left|x'_n - x_n\right|_p, \left|y'_n - y_n\right|_p\right) \to 0$$

per $n \to \infty$. Dunque risulta immediato definire l'inverso additivo di $x = [(x_n)_{n\in\mathbb{N}}]$ come $-x = [(-x_n)_{n\in\mathbb{N}}]$. Mentre per $x \neq 0$, i.e. $|x|_p \neq 0$, si definisce l'inverso moltiplicativo $x^{-1} = [(y_n)_{n\in\mathbb{N}}]$ nel modo seguente: scegliamo un rappresentante per $x$ , $(x'_n)_{n\in\mathbb{N}}$, a termini non nulli. Posso sempre trovarlo: basta prendere $x'_n = x_n$ se $x_n \neq 0$, $x'_n = p^{-n}$ altrimenti, ed avremo

$$\begin{aligned}\left|x'_n - x_n\right|_p &= \begin{cases} 0 & \text{se } x_n \neq 0 \\ p^{-n} & \text{se } x_n = 0 \end{cases} \\ &\leq p^{-n} \to 0\end{aligned}$$

per $n \to \infty$. Poniamo allora $y_n = \frac{1}{x'_n}$ e avremo

$$x^{-1}x = xx^{-1} = [(x_n y_n)_{n\in\mathbb{N}}] = \left[(x'_n y_n)_{n\in\mathbb{N}}\right] = [1]$$

□

**Proposizione 1.2.** *$\mathbb{Q}_p$ per costruzione è completo e $\mathbb{Q}$ è denso in $\mathbb{Q}_p$.*

*Dimostrazione.* $\mathbb{Q}_p$ è completo. Sia infatti $(x^{(k)})_{k\in\mathbb{N}}$ una successione di Cauchy in $\mathbb{Q}_p$. Scelgo dei rappresentanti $(x_n^{(k)})_{n\in\mathbb{N}}$ per ogni $k$. Allora $(x_n^{(k)})_{n\in\mathbb{N}}$ è una successione di Cauchy in $\mathbb{Q}$: per ogni $j$, scelgo un $N_j$ tale che per ogni $i$ e $i' \geq N_j$, $\left|x_i^{(k)} - x_{i'}^{(k)}\right|_p \leq p^{-j}$. Dunque sia $x = (x_{N_k}^{(k)})_{k\in\mathbb{N}}$. Allora $x$ è un elemento di $\mathbb{Q}_p$, cioè una successione di Cauchy in $\mathbb{Q}$, infatti per $h, k \to \infty$ si ha

$$\begin{aligned}\left|x_{N_k}^{(k)} - x_{N_h}^{(h)}\right|_p &= \left|x_{N_k}^{(k)} - x_j^{(k)} + x_j^{(k)} - x_j^{(h)} + x_j^{(h)} - x_{N_h}^{(h)}\right|_p \\ &\leq max\left(\left|x_{N_k}^{(k)} - x_j^{(k)}\right|_p, \left|x_j^{(h)} - x_j^{(k)}\right|_p, \left|x_j^{(h)} - x_{N_h}^{(h)}\right|_p\right) \to 0\end{aligned}$$

dove ho scelto $j$ grande abbastanza tale che $j \geq N_k$, $j \geq N_h$ e $|x^{(h)} - x^{(k)}|_p = |x_j^{(h)} - x_j^{(k)}|_p$. Infine $(x^{(k)})_{k\in\mathbb{N}}$ coverge ad $x$.

$$\begin{aligned}\left|x^{(k)} - x\right|_p &= \lim_n \left|x_n^{(k)} - x_{N_n}^{(n)}\right|_p \\ &= \lim_n \left|x_n^{(k)} - x_{N_k}^{(k)} + x_{N_k}^{(k)} - x_{N_n}^{(n)}\right|_p \\ &\leq max\left(p^{-k}, \lim_n \left|x_{N_k}^{(k)} - x_{N_n}^{(n)}\right|_p\right) \to 0 \quad \text{per } k \to \infty\end{aligned}$$

dove ho usato il fatto che per $n \to \infty$ $n \geq N_k$ e che la successione degli $(x_{N_k}^{(k)})_{k\in\mathbb{N}}$ è di Cauchy.

Inoltre $\mathbb{Q}$ è denso in $\mathbb{Q}_p$. Sia $a \in \mathbb{Q}_p$, allora $a$ è la classe di equivalenza di una successione di Cauchy $(x_n)_{n\in\mathbb{N}}$ in $\mathbb{Q}$. Tale successione converge ad $a$. Infatti $d_p(a, x_n) = p^{-ord_p(a-x_n)}$ e $a - x_n$ è un elemento in $\mathbb{Q}_p$ ($x_n$ è la successione costante uguale ad $x_n$ e un rappresentante per $a - x_n$ in $\mathbb{Q}_p$ è $(x_m - x_n)_{m\in\mathbb{N}}$) e per definizione $ord_p(a - x_n) = ord_p(x_m - x_n)$ per un certo $m \geq M$, con $M$ in $\mathbb{N}$ scelto opportunamente grande, dunque $d_p(a, x_n) = d_p(x_n, x_m)$, che tende a 0 perché la successione $(x_n)_{n\in\mathbb{N}}$ è di Cauchy. □

**Definizione 1.5.** *Si definisce l'anello degli interi p-adici $\mathbb{Z}_p$:*

$$\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid ord_p(a) \geq 0\}$$

**Osservazione 1.3.** *$\mathbb{Z}_p$ è un sottoanello di $\mathbb{Q}_p$ e chiaramente $\mathbb{Z}$ (visto come l'insieme delle successioni costanti di interi) si immerge in $\mathbb{Z}_p$. Si noti che*

$$\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid |a|_p \leq 1\} = B_p[0, 1]$$

*è la palla chiusa unitaria ed è anche aperta. Infatti, per ogni $a \in \mathbb{Z}_p$ tale che $ord_p(a) \geq N \geq 0$ si ha che $B_p[a, p^{-N}) \subseteq \mathbb{Z}_p$. Inoltre sia*

$$\mathbb{Z}_{(p)} = \left\{\frac{a}{b} \mid a, b \in \mathbb{Z} \text{ e } p \text{ non divide } b\right\}$$

*Allora $\mathbb{Z}_{(p)}$ è denso in $\mathbb{Z}_p$ poiché $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)}$.*

Inoltre $\mathbb{Z}$ è denso in $\mathbb{Z}_p$. Vale infatti

**Lemma 1.1.** *Sia $x \in \mathbb{Z}_{(p)}$, cioè $x$ è un razionale con $ord_p(x) \geq 0$. Allora per ogni $k \in \mathbb{N}$ esiste un intero $\alpha \in \mathbb{Z}$ tale che $d_p(x, \alpha) \leq p^{-k}$. In particolare $\alpha \in \{0, 1, 2, ..., p^k - 1\}$.*

*Dimostrazione.* Sia $x = \frac{a}{b}$ in $\mathbb{Z}_{(p)}$. Allora $p$ non divide $b$. Per l'identità di Bezout esistono $n, m \in \mathbb{Z}$ tali che $bm - np^k = 1$. Dunque pongo $\alpha = ma$, vale

$$|x - \alpha|_p = \left|\frac{a}{b} - ma\right|_p = \left|\frac{a}{b}\right|_p |1 - mb|_p \leq \left|np^k\right|_p = p^{-k}$$

Posso aggiungere ad $\alpha$ un multiplo di $p^k$ in modo che $0 \leq \alpha \leq p^k - 1$ e che sussista la disuguaglianza. □

Ciò mostra in particolare che $\mathbb{Z}_p$ è la chiusura di $\mathbb{Z}$ in $\mathbb{Q}_p$. Ci permette inoltre di mostrare il seguente teorema.

**Teorema 1.1.** *Ogni $a \in \mathbb{Z}_p$ ha un unico rappresentante $(a_n)_{n\in\mathbb{N}}$ tale che:*

1. *$0 \leq a_n \leq p^n - 1$ per ogni $n$*
2. *$a_n = a_{n+1} \mod p^n$*

*Dimostrazione.* Mostro l'unicità. Sia $(b_n)_{n\in\mathbb{N}}$ un altro rappresentante per $a$ che verifica la 1. e la 2. diverso da $(a_n)_{n\in\mathbb{N}}$. Allora esiste un $n_0$ tale che $a_{n_0} \neq b_{n_0}$. In particolare poiché $0 \leq a_{n_0}, b_{n_0} \leq p^{n_0} - 1$ si ha che $a_{n_0} \neq b_{n_0} \mod p^{n_0}$. Ma allora per ogni $n \geq n_0$ ho $a_{n_0} = a_n \mod p^{n_0} \neq b_{n_0} = b_n \mod p^{n_0}$ allora $a_n \neq b_n \mod p^{n_0}$ e dunque $p^{n_0}$ non divide

$a_n - b_n$, cioè $d_p(a_n, b_n) \geq p^{-n_0}$ per ogni $n$, il che contraddice il fatto che $d_p(b_n, a_n) \to 0$ perché sono rappresentanti della stessa classe $a$.
Per l'esistenza: fisso un rappresentante $(b_n)_{n\in\mathbb{N}}$ per $a$. La sequenza $(b_n)_{n\in\mathbb{N}}$ è di Cauchy. Scelgo allora, per ogni $k \in \mathbb{N}$, un $N_k$ tale che per $h_1, h_2 \geq N_k$ si ha che $d_p(b_{h_1}, b_{h_2}) \leq p^{-k}$. Non è restrittivo supporre che la successione degli $(N_k)_{k\in\mathbb{N}}$ sia crescente. Si noti che per $h \geq N_1$ si ha che $|b_h|_p \leq 1$, cioè $b_h \in \mathbb{Z}_{(p)}$, infatti

$$|b_h|_p \leq max(|b_h - b_k|_p, |b_k|_p) \leq max(|b_k|_p, p^{-1}) \quad \text{cioè} \quad |b_h| \leq \lim_k |b_k|_p = |a|_p \leq 1$$

Allora applico il Lemma 1.1. e trovo, per ogni $k$, un $a_k$ intero tale che $0 \leq a_k \leq p^{-k} - 1$ e $d_p(a_k, b_{N_k}) \leq p^{-k}$. Allora $(a_k)_{k\in\mathbb{N}}$ è il rappresentante cercato: resta da mostrare che $a_k = a_{k+1} \mod p^k$ e che $\lim_k d_p(a_k, b_k) = 0$. Per la prima si ha:

$$\begin{aligned} |a_k - a_{k+1}|_p &= \left|a_k - b_{N_k} + b_{N_k} - b_{N_{k+1}} + b_{N_{k+1}} - a_{k+1}\right|_p \\ &\leq max\left(|a_k - b_{N_k}|_p, \left|b_{N_k} - b_{N_{k+1}}\right|_p, \left|b_{N_{k+1}} - a_{k+1}\right|_p\right) \\ &\leq max\left(p^{-k}, p^{-k}, p^{-(k+1)}\right) \\ &= p^{-k} \end{aligned}$$

cioè $ord_p(a_k - a_{k+1}) \geq k$ ovvero $p^k$ divide la differenza $a_k - a_{k+1}$, dunque $a_k = a_{k+1} \mod p^k$. Per la seconda, fisso $n \in \mathbb{N}$ allora per ogni $k \geq N_n$ vale:

$$\begin{aligned} d_p(a_k, b_k) &= |a_k - a_n + a_n - b_{N_n} + b_{N_n} - b_k|_p \\ &\leq max\left(|a_k - a_n|_p, |a_n - b_{N_n}|_p, |b_{N_n} - b_k|_p\right) \\ &\leq max\left(p^{-n}, p^{-n}, p^{-n}\right) \\ &= p^{-n} \end{aligned}$$

ovvero $d_p(a_k, b_k) \to 0$ per $k \to \infty$. □

Il teorema ci dice in particolare che un intero $p$-adico in $\mathbb{Z}_p$ è il dato di un elemento in $\lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$, il cui significato verrà presto chiarito.

## 1.2 Definizione algebrica

Introduciamo algebricamente l'anello degli interi $p$-adici $\mathbb{Z}_p$ e $\mathbb{Q}_p$ come il suo campo delle frazioni.

**Definizione 1.6.** *Sia $(X_n)_{n\in\mathbb{N}}$ una sequenza di insiemi e $f_n : X_{n+1} \longrightarrow X_n$ una successione di mappe. Si definisce il limite inverso, $\lim_{\leftarrow} X_n$, del sistema il sottoinsieme di $\prod_{n\geq 1} X_n$*

$$\left\{(a_n)_{n\in\mathbb{N}} \in \prod_{n\geq 1} X_n \mid f_n(a_{n+1}) = a_n\right\}$$

Sia allora, per ogni $n \in \mathbb{N}$, $X_n = \mathbb{Z}/p^n\mathbb{Z}$ l'anello delle classi di interi *mod* $p^n$ e $f_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ la funzione definita ponendo $a_{n+1} \longrightarrow a_n = a_{n+1} \mod p^n$. Si definisce l'anello degli interi $p$-adici:

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \left\{ (a_1, a_2, ..., a_n, a_{n+1}, ...) \in \prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z} \mid a_{n+1} = a_n \mod p^n \right\}$$

L'insieme $\mathbb{Z}_p$ ha la struttura di anello con le operazioni di somma e prodotto definite "componente per componente".
Inoltre l'anello $\mathbb{Z}_p$ è dotato di una topologia. Se dotiamo ciascun $X_n$ della topologia discreta, allora $X_n$ è uno spazio topologico compatto (perché finito) e $\prod_{n\geq 1} X_n$ è dotato della topologia prodotto. Il prodotto $\prod_{n\geq 1} X_n$ è uno spazio topologico compatto e $\mathbb{Z}_p$ eredita la topologia di sottospazio dello spazio prodotto. Infine è chiuso. Sia $(a_1^{(k)}, a_2^{(k)}, ..., a_n^{(k)}, a_{n+1}^{(k)}, ...)_{k\in\mathbb{N}}$ una successione in $\mathbb{Z}_p$ che converge ad un elemento del prodotto $(a_1, a_2, ..., a_n, a_{n+1}, ...) \in \prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$, allora $a_n^{(k)} \to a_n$ e

$$a_{n+1} = \lim_k a_{n+1}^{(k)} = \lim_k f(a_n^{(k)}) = f(\lim_k a_n^{(k)}) = f_n(a_n)$$

(le $f_n$ sono continue perché gli insiemi $X_n$ sono dotati di topologia discreta). Ne consegue che $\mathbb{Z}_p$ è chiuso in un compatto, dunque è compatto.

Valgono:

**Proposizione 1.3.** *Sia $\mathbb{Z}_p$ come nella Definizione 1.6.*

1. *La moltiplicazione per $p^n$ è iniettiva.*
2. *La proiezione $T_n : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ ha nucleo $p^n\mathbb{Z}_p$*

*Dimostrazione.*

1. Basta mostrare che la moltiplicazione per $p$ è iniettiva. Sia $x \in \mathbb{Z}_p$ e $px = 0$. Allora $x = (a_1, a_2, ..., a_n, a_{n+1}, ...)$ e $pa_{n+1} = 0 \mod p^{n+1}$ cioè $a_{n+1}$ è della forma $p^n y_{n+1}$. Ne segue che $a_n = a_{n+1} \mod p^n = 0$ e dunque $a_n = 0\ \forall n$ cioè $x = 0$.

2. Chiaramente se $x = (a_1, .., a_n, a_{n+1}...) \in p^n\mathbb{Z}_p$ allora $a_k = p^n y_k$ per ogni $k$ e di conseguenza $T_n(x) = a_n = 0 \mod p^n$. Viceversa se $T_n(x) = a_n = 0 \mod p^n$ allora si ha $a_m = a_n \mod p^n = 0 \mod p^n\ \forall m \geq n$. Allora per ogni $m$, $\exists\ y_{m-n} \in \mathbb{Z}/p^{m-n}\mathbb{Z}$ tale che $a_m = p^n y_{m-n}$. Dunque $y_i$ definisce un elemento in $\lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$ e verifica $x = p^n y$.

□

**Proposizione 1.4.** *Un elemento $x \in \mathbb{Z}_p$ è invertibile se e solo se $x \notin p\mathbb{Z}_p$. Inoltre ogni $x \in \mathbb{Z}_p$ si scrive come $x = p^n u$ dove $u$ appartiene al gruppo degli invertibili $\mathbb{Z}_p^*$.*

*Dimostrazione.* Per definizione delle operazioni su $\mathbb{Z}_p$, $x = (a_1, a_2, ..., a_n, a_{n+1}...)$ è invertibile se e solo se ciascun $a_n$ lo è in $\mathbb{Z}/p^n\mathbb{Z} = X_n$. Quindi provo la tesi per $X_n$. Ma $x \in X_n = \mathbb{Z}/p^n\mathbb{Z}$ è invertibile se e solo se è coprimo con $p^n$ se e solo se $p$ non divide $x$ se e solo se $x \notin pX_n$. Sia infine $x \in \mathbb{Z}_p$, diverso da 0. Se $x$ non è invertibile esiste un $n$ tale che $T_n(x) = a_n$ è zero dunque $x = p^n u$ con $u$ invertibile. □

Possiamo allora definire la valutazione $p$-adica di $x \in \mathbb{Z}_p$:

**Definizione 1.7.** *Sia $x = p^n u$ con $u$ invertibile e $x \neq 0$ si pone $ord_p(x) = n$. Infine $ord_p(0) = \infty$.*

A questo punto possiamo descrivere la topologia *su* $\mathbb{Z}_p$.

**Proposizione 1.5.** *La topologia su $\mathbb{Z}_p$ è descritta dalla distanza:*

$$d_p(x, y) = p^{-ord_p(x-y)}$$

*$\mathbb{Z}_p$ è uno spazio metrico completo.*

*Dimostrazione.* Una base di intorni di 0 in $\mathbb{Z}_p$ è data da $p^n\mathbb{Z}_p$, dunque un elemento $x \in p^n\mathbb{Z}_p$ se e solo se $ord_p(x) \geq n$ se e solo se $d_p(x, 0) \leq p^{-n}$, dunque $d_p$ definisce la topologia su $\mathbb{Z}_p$. D'altro lato $\mathbb{Z}_p$ è compatto per quanto mostrato sopra, dunque completo. □

**Definizione 1.8.** *Il campo degli numeri $p$-adici $\mathbb{Q}_p$ è il campo delle frazioni di $\mathbb{Z}_p$ ovvero*

$$\mathbb{Q}_p = \left\{xy^{-1} \mid x, y \in \mathbb{Z}_p\right\} = \mathbb{Z}_p[p^{-1}]$$

In particolare un elemento (diverso da zero) in $\mathbb{Q}_p$ è descritto da $p^n u(p^m v)^{-1} = p^k w$ dove $u, v \in \mathbb{Z}_p^*$, $w = uv^{-1} \in \mathbb{Z}_p^*$ e $k = n - m \in \mathbb{Z}$. Posso allora estendere la valuatzione $p$-adica a $\mathbb{Q}_p$, ponendo, se $x = p^m u$, dove $m \in \mathbb{Z}$ e u invertibile in $\mathbb{Z}_p$, $ord_p(x) = m$. In particolare avremo $ord_p(x) \geq 0$ se e solo se $x \in \mathbb{Z}_p$.

## 1.3 Equivalenza delle definizioni

Sia $\mathbb{Z}_p$ come nella Definizione 1.5.

**Teorema 1.2.** *Vale l'equivalenza*

$$\mathbb{Z}_p \simeq \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

*Dimostrazione.* Un elemento $(a_1, a_2, ..., a_n, a_{n+1}...)$ del limite inverso rappresenta una successione di Cauchy in $\mathbb{Q}$. Sia $\forall n \in \mathbb{N}$, $x_n$ intero tale che l'immagine di $x_n$ in $\mathbb{Z}/p^n\mathbb{Z}$ sia $a_n$. Allora $(x_n)_{n\in\mathbb{N}}$ è di Cauchy: fissato $N \in \mathbb{N}$, per ogni $n, m \geq N$, ho che $a_n = a_N \mod p^N$ e $a_m = a_N \mod p^N$ dunque

$$a_N = x_n \mod p^N = x_m \mod p^N \text{ ovvero } x_n = x_m \mod p^N$$

che implica che $p^N$ divide $x_n - x_m$ cioè $d_p(x_n, x_m) \leq p^{-N}$. Viceversa, per il Teorema 1.1 ad ogni intero $p$-adico possiamo associare un elemento di $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ in maniera univoca, scegliendo un opportuno rappresentate. Chiaramente le corrispondenze così definite sono una l'inversa dell'altra. □

## 1.4 Rappresentazione degli interi $p$-adici

Ogni elemento $a \in \mathbb{Z}_p$ può essere rappresentato come

$$a = a_0 + a_1 p + ... + a_n p^n + ...$$

dove $a_i \in \{0, 1, 2, ..., p-1\}$. Infatti sia $x_n = a \mod p^n$ allora $x_n = a_0 + a_1 p + ... + a_{n-1} p^{n-1}$ e chiaramente appartiene a $\mathbb{Z}/p^n\mathbb{Z}$. Dunque $x_{n-1} = a_0 + a_1 p + ... + a_{n-2} p^{n-2}$ e $x_n = x_{n-1} \mod p^{n-1}$. Così ad $a$ associamo un elemento del limite inverso $(x_i)_{i \in \mathbb{N}}$.
Diremo allora che $a = b \mod p^n$ se $|a - b|_p \leq p^{-n}$ ovvero $a - b \in p^n \mathbb{Z}_p$, quindi la prima cifra non nulla dell'espansione sopra è l'$n$-esima.

## 1.5 Soluzioni di equazioni $p$-adiche

Sia $f \in \mathbb{Z}_p[X_1, ..., X_m]$ un polinomio a coefficienti nell'anello degli interi $p$-adici. Denotiamo con $f_n$ il polinomio a coefficienti in $\mathbb{Z}/p^n\mathbb{Z}$ ottenuto riducendo $f$ modulo $p^n$.

**Lemma 1.2.** *Sia $f \in \mathbb{Z}_p[X_1, ..., X_m]$. Le seguenti sono equivalenti:*

1. *$f$ ha uno zero in $\mathbb{Z}_p^m$ cioè esiste $a = (a_1, .., a_m) \in \mathbb{Z}_p^m$ tale che $f(a) = 0$*
2. *$f_n$ ha uno zero in $\mathbb{Z}/p^n\mathbb{Z}$ per ogni $n$ cioè l'equazione $f(X) = 0 \mod p^n$ ha soluzione per ogni $n$.*

*Dimostrazione.* Se $f$ ha uno zero $a = (a_1, ..., a_m) \in \mathbb{Z}_p^m$ si ha che $0 = f(a) = f(a) \mod p^n = f_n(a \mod p^n)$. Viceversa sia, per ogni $n$, $a^{(n)} = (a_1^{(n)}, ..., a_m^{(n)}) \in \mathbb{Z}_p^m$ una soluzione di $f(X) = 0 \mod p^n$. Allora $a^{(n)}$ è una successione in $\mathbb{Z}_p^m$ che verifica $f(a^{(n)}) \mod p^k = 0 \; \forall k \leq n$. Dunque, ricordando che $\mathbb{Z}_p$ è compatto, a meno di sottosuccessioni, $a^{(n)}$ converge ad un elemento in $\mathbb{Z}_p$, $y$, che è uno zero di $f$, poiché verifica $f(y) = f(a^{(n)}) \mod p^n = 0 \mod p^n$ per ogni $n$, cioè $|f(y)|_p \leq p^{-n}$ per ogni $n$, se e solo se $|f(y)|_p = 0$ dunque $f(y) = 0$. □

Si dice che $x = (x_1, ..., x_m) \in \mathbb{Z}_p^m$ è *primitivo* se una delle $x_i$ è invertibile, cioè non tutte le $x_i \in p\mathbb{Z}_p$. Allo stesso modo si definisce un elemento primitivo in $(\mathbb{Z}/p^n\mathbb{Z})^m$ .

**Lemma 1.3.** *Sia $f \in \mathbb{Z}_p[X_1, X_2, ...X_m]$ un polinomio omogeneo a coefficienti in $\mathbb{Z}_p$. Le seguenti sono equivalenti:*

1. *$f$ ha uno zero in $\mathbb{Q}_p^m$ non banale*
2. *$f$ ha uno zero primitivo in $\mathbb{Z}_p^m$*
3. *$f(X) = 0 \mod p^n$ ha una soluzione primitiva per ogni $n$*

*Dimostrazione.* La doppia implicazione 2. $\Leftrightarrow$ 3. segue dal Lemma 1.2. Sia ora $x = (x_1, ..., x_m)$ uno zero non banale di $f$. Sia $k = \min_i ord_p(x_i)$ e pongo $y_i = p^{-k} x_i$. Allora $y = (y_1, ..y_m)$ verifica $ord_p(y_i) \geq 0$ ed esiste $i$ tale che $ord_p(x_i) = 0$, cioè $y$ è primitivo in $\mathbb{Z}_p$. Chiaramente è ancora una soluzione di $f$. Ciò mostra 1. $\Leftrightarrow$ 2. □

Vogliamo ora passare da una soluzione $\mod p^n$ di $f$ ad una "vera" soluzione di $f$ a coefficienti in $\mathbb{Z}_p$.

**Teorema 1.3** (Lemma di Hensel)**.** *Ogni zero semplice della riduzione modulo $p$ di un polinomio $f(X_1, ..., X_m)$ a coefficienti in $\mathbb{Z}_p$ può essere sollevato ad uno zero di $f$ in $\mathbb{Z}_p^m$.*

La dimostrazione del teorema si basa sul lemma:

**Lemma 1.4.** *Sia $f \in \mathbb{Z}_p[X]$ e sia $f'$ la sua derivata. Siano $x \in \mathbb{Z}_p$, $n$ e $k$ interi tali che $0 \leq 2k < n$ e $f(x) = 0 \mod p^n$ e $ord_p(f'(x)) = k$. Allora esiste $y \in \mathbb{Z}_p$ tale che*

$$f(y) = 0 \mod p^{n+1}, \quad ord_p(f'(y)) = k \quad e \quad y = x \mod p^{n-k}$$

*Dimostrazione.* Cerco $y$ della forma $y = x + zp^{n-k}$ con $z \in \mathbb{Z}_p$ tale che $f(y) = 0 \mod p^{n+1}$. Sviluppando secondo la formula di Taylor otteniamo:

$$f(y) = f(x) + f'(x)p^{n-k}z + ap^{2(n-k)}$$

con $a \in \mathbb{Z}_p$. Allora so che $f(x) = 0 \mod p^n$ e $ord_p(f'(x)) = k$, cioè $f(x) = bp^n$ e $f'(x) = cp^k$ dunque $f(y) = 0 \mod p^{n+1}$ se e solo se

$$bp^n + czp^k p^{n-k} + ap^{2(n-k)} = 0 \mod p^{n+1} \Leftrightarrow b + cz = 0 \mod p$$

(osservo che sotto le ipotesi del lemma $2n-2k \geq n$). Quindi $z$ è univocamente determinato e verifica $f(y) = f(x + p^{n-k}z) = 0 \mod p^{n+1}$.
Infine applicando Taylor ad $f'$ abbiamo $f'(y) = cp^k + wp^{n-k}$ per qualche $w \in \mathbb{Z}_p$ e da $n - k > k$ otteniamo $ord_p(f'(y)) = k$. □

Possiamo ora mostrare il Teorema 1.3. Quest'ultimo equivale a dimostrare che, dato un polinomio $f(X_1, X_2, ..., X_m) \in \mathbb{Z}_p[X_1, ..., X_m]$ e $x = (x_1, ..., x_m) \in (\mathbb{Z}_p)^m$ tale che $f(x_1, ..., x_m) = 0 \mod p$ ed esiste j con $0 \leq j \leq m$ tale che $f_{X_j}(x) \neq 0 \mod p$, allora esiste uno zero $y = (y_1, ..., y_m) \in (\mathbb{Z}_p)^m$ di $f$ tale che $y_i = x_i \mod p$.

*Dimostrazione.* Sia $m = 1$. Allora $f = f(X) \in \mathbb{Z}_p[X]$ verifica $f(x) = 0 \mod p$ e $f'(x) \neq 0 \mod p$. Siamo sotto le ipotesi del Lemma 1.4. con $n = 1$ e $k = 0$ (da $f'(x) \notin p\mathbb{Z}_p$ ho che $ord_p(f'(x)) = 0$ e in particolare è invertibile). Allora pongo $x^{(1)} = x$ e trovo $x^{(2)} \in \mathbb{Z}_p$ tale che $f(x^{(2)}) = 0 \mod p^2$ e $x^{(2)} = x^{(1)} \mod p$. Applichiamo nuovamente il Lemma 1.4. ad $x^{(2)}$ con $n = 2$ e $k = 0$ e troviamo $x^{(3)}$. Procediamo iterativamente e costruiamo una successione $x^{(1)}, x^{(2)}, ..., x^{(h)}, ..$ di elementi in $\mathbb{Z}_p$ tali che

$$x^{(h+1)} = x^{(h)} \mod p^h, \quad f(x^{(h)}) = 0 \mod p^h$$

Allora dalla prima otteniamo che $x^{(h)}$ è una successione di Cauchy in $\mathbb{Z}_p$ che è completo. Sia $y$ il suo limite, allora $f(y) = 0$ e $y = x \mod p$.
Per il caso $m > 1$ ci si riconduce al caso m=1 lavorando su $x_j$. Nello specifico si consideri il polinomio $\tilde{f} \in \mathbb{Z}_p[X_j]$ in una variabile che si ottiene ponendo $f(x_1, .., X_j, ..., x_m) = \tilde{f}(X_j)$ e si applichi il ragionamento di sopra ad $\tilde{f}$ e ad $x_j$. Si trova $y_j$ zero di $\tilde{f}$ con $y_j = x_j \mod p$ e si pone $y_i = x_i$ per $i \neq j$, il che permette di concludere. □

**Corollario 1.1.** *Sia $p \neq 2$. Sia $f(X) = \sum_{i,j} a_{ij} X_i X_j$ una forma quadratica a coefficienti in $\mathbb{Z}_p$ tale che $det(a_{ij})$ è invertibile. Sia $a \in \mathbb{Z}_p$. Allora ogni soluzione primitiva di $f(X) = a \mod p$ si solleva ad una vera soluzione.*

*Dimostrazione.* Basta mostrare che ogni soluzione $x$ primitiva di $f(X) = a \mod p$ è uno zero semplice, cioè esiste $X_j$ tale che $f_{X_j}(x) \neq 0 \mod p$. Ma $f_{X_i}(X) = 2\sum_j a_{ij} X_j$ e poiché $x$ è primitiva e $det(a_{ij}) \neq 0 \mod p$ l'ipotesi è verificata. □

**Corollario 1.2.** *Sia $p = 2$. Sia $f(X) = \sum_{i,j} a_{ij} X_i X_j$ una forma quadratica a coefficienti in $\mathbb{Z}_2$ e sia $a \in \mathbb{Z}_2$ e $x$ una soluzione primitiva di $f(X) = a \mod 8$. Se almeno una delle $f_{X_j}(x) \mod 4$ è non nulla, allora $x$ si solleva ad una vera soluzione in $\mathbb{Z}_2$.*

*Dimostrazione.* Sia $j$ tale che $f_{X_j}(x) \mod 4$ è non nulla. Come sopra costruisco il polinomio $\tilde{f}(X_j) = f(x_1, x_2 ..., X_j, ...x_n) - a$. Allora $\tilde{f}(x_j) = 0 \mod 8$ e $\tilde{f}'(x_j) \neq 0 \mod 4$. Siamo sotto le ipotesi del Lemma 1.4 con $n = 3$ e $k = ord_p(\tilde{f}'(x_j)) < 2$. Posto $x_j = x_j^{(1)}$ trovo allora una $x_j^{(2)}$ tale che $\tilde{f}(x_j^{(2)}) = 0 \mod 16$, $x_j^{(2)} = x_j^{(1)} \mod 2^{3-k}$ e $ord_p(\tilde{f}'(x_j^{(2)})) = k$. Procedo applicando iterativamente lo stesso argomento e come nella dimostrazione del Teorema 1.3. ottengo una successione $x_j^{(1)}, x_j^{(2)}, ..., x_j^{(m)}, ...$ tale che

$$x_j^{(m+1)} = x_j^{(m)} \mod 2^{m+2-k} \text{ e } f(x_j^{(m)}) = 0 \mod 2^{m+2}$$

Come sopra, tale successione converge ad uno zero $y_j$ di $\tilde{f}$ tale che $y_j = x_j \mod 2^{3-k}$ e, ricordando che $3 - k > 1$, $y_j = x_j \mod 2$. Posto $y_i = x_i$ per $i \neq j$, allora $y$ è un sollevamento di $x$ e ciò conclude la dimostrazione. □

## 1.6 La struttura di $\mathbb{Q}_p^*$

Sia $\mathbb{Q}_p^* = \mathbb{Q}_p \setminus \{0\}$ il gruppo degli invertibili del campo dei numeri $p$-adici. Vogliamo descrivere $\mathbb{Q}_p^*$ in termini di gruppi noti.

**Lemma 1.5.** *$\mathbb{Q}_p^* \simeq \mathbb{Z} \times \mathbb{Z}_p^*$ dove $\mathbb{Z} \simeq (\mathbb{Z}, +)$ gruppo additivo e $\mathbb{Z}_p \simeq (\mathbb{Z}_p, *)$ gruppo moltiplicativo.*

*Dimostrazione.* Dalla Definizione 1.8. si ha che ogni elemento $a \in \mathbb{Q}_p$ si scrive in modo unico come $a = p^n u$ dove $a \in \mathbb{Z}$ e $u$ invertibile in $\mathbb{Z}_p$. Chiaramente la scrittura rispetta le operazioni di gruppo, dunque la biiezione così definita è isomorfismo di gruppi. □

**Lemma 1.6.** *$\mathbb{Z}_p^* \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times (1 + p\mathbb{Z}_p)$ con $\mathbb{Z}/(p-1)\mathbb{Z} \simeq \mathbb{F}_p^*$ il gruppo degli invertibili del campo con $p$ elementi. In particolare $\mathbb{Z}_2^* \simeq 1 + 2\mathbb{Z}_2$.*

*Dimostrazione.* Considero l'applicazione $f : \mathbb{Z}_p^* \longrightarrow \mathbb{F}_p^*$ definita ponendo $f(x) = x \mod p$. Allora $f$ è la funzione che manda l'elemento $x = a_0 + a_1 p + ... + a_n p^n + ...$ di $\mathbb{Z}_p^*$ in $a_0 \in \{1, 2, ..., p-1\} = \mathbb{F}_p^*$. Si mostra che $f$ è suriettiva: sia $a \in \mathbb{F}_p^*$ e si consideri il polinomio $g(X) = X^{p-1} - 1$. Chiaramente $a$ è uno zero semplice di $g(X)$, allora si solleva ad una $x \in \mathbb{Z}_p$ tale che $x = a \mod p$ e $x^{p-1} = 1$, cioè $x$ è invertibile e $f(x) = a$. Inoltre $f$ è un omomorfismo di gruppi. Siano infatti $a, b \in \mathbb{Z}_p^*$, allora $a = a_0 + a_1 p + ... + a_n p^n + ...$ e $b = b_0 + b_1 p + ... + p_n p^n + ...$ con $a_0, b_0 \in \mathbb{F}_p^*$ e $a_0 = a \mod p$ e $b_0 = b \mod p$. Allora

$ab = a_0b_0 + (a_0b_1 + a_1b_0)p + ...$ e $f(ab) = ab \mod p = a_0b_0 = f(a)f(b)$. Per concludere basta mostrare che il nucleo di $f$ è $1 + p\mathbb{Z}p$: chiaramente $1 + px$ con $x \in \mathbb{Z}_p$ ha immagine $1 \in \mathbb{F}_p^*$. Viceversa sia $f(a) = a \mod p = 1 \mod p$ allora $a = 1 + px$ con $x \in \mathbb{Z}_p$ cioè $a \in 1 + p\mathbb{Z}_p$. □

**Lemma 1.7.** *Se $p \neq 2$, $(1 + p\mathbb{Z}_p) \simeq \mathbb{Z}_p$.*
*Se $p = 2$, $(1 + 2\mathbb{Z}_2) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$.*

Per mostrare il Lemma 1.7 introduciamo le funzioni $exp(x)$ e $log(x)$.

**Osservazione 1.4.** *Sia $\sum_n a_n$ una serie di elementi in $\mathbb{Z}_p$. Allora la serie converge se e solo se $|a_n|_p \to 0$ per $n \to \infty$ se e solo se $ord_p(a_n) \to \infty$ per $n \to \infty$.*

Infatti, detta $s_n$ la serie delle ridotte, si ha che $s_n$ converge $p$-adicamente se e solo se è di Cauchy. Ma per le proprietà di $|-|_p$

$$|s_n - s_m|_p = \left|\sum_{k=n}^{m} a_n\right|_p \leq \max_{k=n,...,m}(|a_k|_p)$$

e poiché $|a_k|_p \to 0$ si conclude.

**Definizione 1.9.** *Definiamo:*

$$exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \quad \text{per } x \in p\mathbb{Z}_p \text{ se } p \neq 2 \text{ e per } x \in 4\mathbb{Z}_2 \text{ se } p = 2.$$

$$log(x) = \sum_{n=1}^{\infty} \frac{(-1)^n}{n}(x-1)^n \quad \text{per } x - 1 \in p\mathbb{Z}_p.$$

I domini di definizione di $exp(x)$ e $log(x)$ sono esattamente $p\mathbb{Z}_p$ e $1 + p\mathbb{Z}_p$. Ciò segue dalla proposizione:

**Proposizione 1.6.** *Valgono:*

1. *Per ogni $n > 0$, sia $n = a_0p + a_1p + ... + a_kp^k$, la scrittura di $n$ in base $p$. Allora:*

$$ord_p(n!) = \frac{n - S_n}{p - 1}$$

*dove $S_n = a_0 + a_1 + ... + a_k$. In particolare si ha che $ord_p(n!) \leq \frac{n-1}{p-1}$.*

2. *Sia $c \in \mathbb{R}$. Allora $nc - ord_p(n!) \to \infty$ per $n \to \infty$ se e solo se $c > \frac{1}{p-1}$. Inoltre $nc - ord_p(n) \to \infty$ per $n \to \infty$ se e solo se $c > 0$.*

3. *se $c > \frac{1}{p-1}$ per ogni $n \geq 1$ si ha $nc - ord_p(n!) \geq c$*

*Dimostrazione.* 1. Vale che $ord_p(n) = m$ se e solo se $a_i = 0$ per $i \leq m$ e $a_m \neq 0$. Ora

$$\begin{aligned} n - 1 &= a_0p + a_1p + ... + a_kp^k - 1 = a_mp^m + ... + a_kp^k - 1 \\ &= (p-1) + (p-1)p + (p-1)p^2 + ... + (p-1)p^{m-1} + (a_m - 1)p^m + ... + a_kp^k \end{aligned}$$

Dunque $S_{n-1} = a_m - 1 + ... + a_k + (p-1)m$ e da qui $m = \frac{S_{n-1}-S_n+1}{p-1}$.
Segue che

$$ord_p(n!) = \sum_{k=1}^{n} ord_p(k) = \sum_{k=1}^{n} \frac{S_{k-1} - S_k + 1}{p-1} = \frac{n - S_n}{p-1}$$

Chiaramente se $n \neq 0$, $S_n \geq 1$ e allora $ord_p(n!) \leq \frac{n-1}{p-1}$.

2. Dal punto precedente segue che

$$nc - ord_p(n!) \geq nc - \frac{n}{p-1} = n\left(c - \frac{1}{p-1}\right) \to \infty$$

se $c > \frac{1}{p-1}$. Sia d'altra parte $n = p^m$, allora

$$nc - ord_p(n!) = nc - \frac{n-1}{p-1} = n\left(c - \frac{1}{p-1}\right) + \frac{1}{p-1} \to \infty$$

per $n \to \infty$ se e solo se $c > \frac{1}{p+1}$ . Analogamente, osservando che $ord_p(n) \leq \log_p(n)$ (dove $\log_p$ è la funzione reale), si ha

$$nc - ord_p(n) \geq nc - log_p(n) \to \infty$$

se $c > 0$. Ponendo $n = p^m$ si ottiene $nc - ord_p(n) = nc - log_p(n) \to 0$ per $n \to \infty$ se e solo se $c > 0$.

3. Infine se $c > \frac{1}{p-1}$ e $n \neq 0$ si ha

$$nc - ord_p(n!) - c \geq nc - \frac{n-1}{p-1} - c = (n-1)\left(c - \frac{1}{p-1}\right) \geq 0$$

□

Dunque $exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$ converge se e solo se

$$ord_p\left(\frac{x^n}{n!}\right) = ord_p(x)n - ord_p(n!) \to \infty \quad \text{se e solo se } ord_p(x) > \frac{1}{p-1}$$

Allora se $p \neq 2$ ho $ord_p(x) \geq 1$ cioè $x \in p\mathbb{Z}_p$, altrimenti $ord_2(x) > 1$ e $x \in 4\mathbb{Z}_2$. Allo stesso modo $log(x) = \sum_{n=1}^{\infty} \frac{(-1)^n}{n}(x-1)^n$ converge se e solo se

$$ord_p\left(\frac{(-1)^n}{n}(x-1)^n\right) = ord_p(x-1)n - ord_p(n) \to \infty \quad \text{se e solo se } ord_p(x-1) > 0$$

Ne consegue che $log(x)$ è definito se e solo se $ord_p(x-1) \geq 1$, cioè $x - 1 \in p\mathbb{Z}_p$.
Sia allora $x \in p^m\mathbb{Z}_p$. Dunque $exp(x) = 1 + \sum_{n=1}^{\infty} \frac{x^n}{n!}$. Si noti che

$$ord_p\left(\frac{x^n}{n!}\right) = ord_p(x)n - ord_p(n!) \geq ord_p(x) = m$$

per ogni $n \geq 1$ per la 3. della Proposizione 1.4. Allora $\sum_{n=1}^{\infty} \frac{x^n}{n!}$ ha ordine maggiore o uguale ad $m$, cioè $exp(x) \in (1 + p^m\mathbb{Z}_p)$ . Viceversa se $x \in (1 + p^m\mathbb{Z}_p)$

$$ord_p\left(\frac{(-1)^n}{n}(x-1)^n\right) = ord_p(x-1)n - ord_p(n) \geq ord_p(x-1)n - ord_p(n!)$$
$$\geq ord_p(x-1) = m$$

cioè $log(x) \in p^m\mathbb{Z}_p$.
Inoltre, come nel caso reale e complesso, $exp(x)$ e $log(x)$ sono l'una l'inversa dell'altra e verificano le proprietà $exp(x+y) = exp(x)exp(y)$ e $log(xy) = log(x) + log(y)$. Quindi le due permettono di costruire l'isomorfismo:

$$p^m\mathbb{Z}_p \simeq (1 + p^m\mathbb{Z}_p) \tag{1.1}$$

Tornando al Lemma 1.7, possiamo ora mostrarlo:

*Dimostrazione.* Se $p \neq 2$, si ha $p\mathbb{Z}_p \simeq (1 + p\mathbb{Z}_p)$ per la (1.1). Dalla 1 della Proposizione 1.3 otteniamo $\mathbb{Z}_p \simeq p\mathbb{Z}_p$.
Se $p = 2$, consideriamo l'omomorfismo di gruppi $\mathbb{Z}_2^* = (1 + 2\mathbb{Z}_2) \longrightarrow (\mathbb{Z}/4\mathbb{Z})^*$, definito ponendo: $x = 1 + 2a_1 + 4a_2 + ... \longrightarrow 1 + 2a_1 = x \mod 4$ . Allora tale applicazione ha nucleo $(1 + 4\mathbb{Z}_2)$ ed immagine $\{1, 3\} \simeq \mathbb{Z}/2\mathbb{Z} \subseteq \mathbb{Z}/4\mathbb{Z}$, dunque induce la decomposizione $(1+2\mathbb{Z}_2) \simeq \mathbb{Z}/2\mathbb{Z} \times (1+4\mathbb{Z}_2)$. Dalla (1.1) ho $4\mathbb{Z}_2 \simeq (1+4\mathbb{Z}_2)$ e dalla 1 della Proposizione 1.3 trovo che $\mathbb{Z}_2 \simeq 4\mathbb{Z}_2$, il che permette di concludere. □

I lemmi precedenti ci permettono di enunciare la seguente proposizione:

**Proposizione 1.7.**

$$Se\ p \neq 2 \quad \mathbb{Q}_p^* \simeq \mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$$
$$Se\ p = 2 \quad \mathbb{Q}_2^* \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$$

## 1.7 I quadrati in $\mathbb{Q}_p^*$

Enunciamo il seguente risultato preliminare

**Lemma 1.8.** *Sia p primo, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ il campo con p elementi. Se $p = 2$ tutti gli elementi di $\mathbb{F}_2$ sono quadrati. Se $p \neq 2$ i quadrati di $\mathbb{F}_p^*$ formano un sottogruppo di indice 2. In particolare $\mathbb{F}_p^{*2}$ è il nucleo dell'omomorfismo*

$$\mathbb{F}_p^* \longrightarrow \{+1, -1\}$$
$$x \longrightarrow x^{\frac{p-1}{2}}$$

*Dimostrazione.* Il caso $p = 2$ segue dal fatto che $x^2 = x$ in $\mathbb{Z}/2\mathbb{Z}$. Sia $p \neq 2$ e $x \in \mathbb{F}_p$. Sia $\Omega \supseteq \mathbb{F}_p$ una opportuna estensione di $\mathbb{F}_p$ e $y \in \Omega$ tale che $y^2 = x$. Allora l'elemento $y^{(p-1)} = x^{\frac{p-1}{2}} \in \{+1, -1\}$ poiché $x \in \mathbb{Z}/p\mathbb{Z}$. In particolare $y \in \mathbb{F}_p$ se e solo se ha ordine $p - 1$, cioè $y^{(p-1)} = 1$ se e solo se $x^{\frac{p-1}{2}} = 1$. Allora $\mathbb{F}_p^{*2}$ è il nucleo dell'omomorfismo di cui sopra, cioè $\mathbb{F}_p^*/\mathbb{F}_p^{*2} \simeq \{1, -1\}$ e ciò conclude la dimostrazione. □

**Proposizione 1.8.** *Sia $p \neq 2$ e $x \in \mathbb{Q}_p^*$. Sia $x = p^m u$ con $m \in \mathbb{Z}$ e $u \in \mathbb{Z}_p^*$ la sua decomposizione in $\mathbb{Z} \times \mathbb{Z}_p^*$. Allora $x$ è un quadrato in $\mathbb{Q}_p^*$ se e solo se*

1. *$m$ è pari*
2. *$u \mod p$ è un quadrato in $\mathbb{F}_p^*$*

*In particolare $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

*Dimostrazione.* L'elemento $x = p^m u$ in $\mathbb{Q}_p$ è un quadrato se e solo se $m$ è pari e $u$ è un quadrato in $\mathbb{Z}_p^*$. Sia $u = vy$ la sua decomposizione in $\mathbb{F}_p^* \times (1 + p\mathbb{Z}_p)$. Allora $u$ è un quadrato se e solo se $v$ ed $y$ lo sono. Si noti che tutti gli elementi in $1+p\mathbb{Z}_p$ sono quadrati. Infatti sia $a \in (1 + p\mathbb{Z}_p)$ e $f(X) = X^2 - a$. Allora $f \mod p$ ha lo zero semplice 1 in $\mathbb{Z}_p$. Per il Teorema 1.3 tale radice si solleva ad uno zero di $f$ in $\mathbb{Z}_p$, $b$, tale che $b = 1 \mod p$. Ma allora $b \in (1 + p\mathbb{Z}_p)$ e $b^2 = a$.
Ne consegue che $u$ è un quadrato se e solo se la sua immagine $y \in \mathbb{F}_p^*$ lo è se e solo se $u \mod p$ è un quadrato in $\mathbb{F}_p^*$. Dunque è evidente la decomposizione

$$\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{*2} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

□

**Proposizione 1.9.** *Un elemento $x \in \mathbb{Q}_2^*$ , $x = 2^n u$, con $n \in \mathbb{Z}$ e $u \in \mathbb{Z}_2^*$, è un quadrato se e solo se*

1. *$n$ è pari*
2. *$u = 1 \mod 8$*

*Inoltre $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

*Dimostrazione.* L'elemento $x = 2^n u$ è un quadrato se e solo se $n$ è pari e $u$ è un quadrato in $\mathbb{Z}_2^* \simeq (1 + 2\mathbb{Z}_2)$. D'altro lato $u$ è un quadrato se e solo se l'equazione $f(X) = X^2 - u$ ha una soluzione in $\mathbb{Z}_p^*$. Se $u \in (1 + 8\mathbb{Z}_2)$, allora $f(x) \mod 8$ ha una soluzione, 1, tale che $f'(1) \neq 0 \mod 4$. Siamo dunque sotto le ipotesi del Corollario 1.2: la soluzione 1 si solleva ad uno zero di $f$, $b \in \mathbb{Z}_2^*$, che verifica $b^2 = u$. Viceversa se $u$ è un quadrato in $(\mathbb{Z}_2)^*$ allora $u \in \{1, 3, 5, 7\} \mod 8$ perchè invertibile e l'unico quadrato tra questi è 1, il che permette di concludere che $u = 1 \mod 8$.
Infine $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2^*/(1 + 8\mathbb{Z}_2)$ e $\mathbb{Z}_2^*/(1 + 8\mathbb{Z}_2) \simeq (\mathbb{Z}/8\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ tramite la riduzione modulo 8, il che permette di concludere. □

# Capitolo 2

# La legge di reciprocità quadratica e il simbolo di Hilbert

## 2.1 Equazioni su un campo finito

Sia $\mathbb{F}_q$ il campo con $q = p^m$ elementi. Enunciamo il seguente lemma preliminare:

**Lemma 2.1.** *Sia $u$ un intero. La somma $S(X^u) = \sum_{x \in \mathbb{F}_q} x^u$ è uguale a $-1$ se $q-1$ divide $u$, è uguale a zero altrimenti.*

*Dimostrazione.* Sia $u = 0$, allora $x^u = 1$ per ogni $x \in \mathbb{F}_q$ e $S(X^u) = q \cdot 1 = 0$. Sia $u \neq 0$ e divisibile per $q-1$. Allora se $x \neq 0$ e $x \in \mathbb{F}_q$ si ha $x^u = x^{q-1} = 1$, dunque $S(X^u) = \sum_{x \in \mathbb{F}_q^*} x^u = q - 1 = -1$. Infine sia $u$ non divisibile per $q-1$, allora esiste $y \in \mathbb{F}_q$ tale che $y^u \neq 1$. Vale

$$S(X^u) = \sum_{x \in \mathbb{F}_q} x^u = \sum_{x \in \mathbb{F}_q} x^u y^u = y^u \sum_{x \in \mathbb{F}_q} x^u = y^u S(X^u)$$

se e solo se $S(X^u)(1 - y^u) = 0$ se e solo se $S(X^u) = 0$. □

**Teorema 2.1** (Chevalley-Warning)**.** *Siano $f_\alpha$ dei polinomi in $n$ variabili con la condizione sui gradi: $\sum_\alpha deg(f_\alpha) < n$. Sia $V$ l'insieme dei loro zeri comuni. Allora*

$$card(V) = 0 \mod p$$

*Dimostrazione.* Sia $P(X) = \prod_\alpha (1 - f_\alpha^{q-1})$. Se $x \in V$ per ogni $\alpha$ ho $f_\alpha(x) = 0$ e $P(x) = 1$, mentre se $x \notin V$ almeno uno degli $f_\alpha$ è diverso da zero e verifica $f_\alpha^{q-1} = 1$ e allora $P(x) = 0$, cioè $P$ è la funzione caratteristica di $V$. Allora

$$card(V) \mod p = \sum_{x \in (\mathbb{F}_q)^n} P(x) = S(P(X))$$

Quindi basta mostrare che $S(P(X)) = 0$. Si noti che, poiché $\sum_\alpha deg(f_\alpha) < n$, $P(X)$ ha grado uguale a $\sum_\alpha (q-1) deg(f_\alpha) < (q-1)n$. Allora $P(X)$ sarà combinazione di monomi del tipo $X^u = X_1^{u_1} X_2^{u_2} ... X_n^{u_n}$ con $\sum_{i=1}^n u_i < n(q-1)$ cioè almeno uno degli $u_i$ è minore di $q-1$. Quindi ciascun monomio $X^u$ verifica $S(X^u) = 0$ per il Lemma 2.1 e si conclude. □

**Corollario 2.1.** *Sia $f_\alpha$ una famiglia di polinomi in $n$ variabili con $\sum_\alpha deg(f_\alpha) < n$, ciascuno con termine noto nullo. Allora gli $f_\alpha$ hanno una soluzione comune distinta da quella banale.*

*Dimostrazione.* Sia $V$ l'insieme degli zeri comuni degli $f_\alpha$. Se fosse $V = \{0\}$, si avrebbe $card(V) = 1$ che contraddice il Teorema 2.1. Dunque $V$ contiene necessariamente almeno un altro elemento. □

Il corollario si applica al caso in cui gli $f_\alpha$ sono polinomi omogenei. In particolare vale il seguente corollario:

**Corollario 2.2.** *Ogni forma quadratica in $n$ variabili, $f(X_1, X_2, ..., X_n) = \sum_{i,j=1}^{n} a_{ij} X_i X_j$, su $\mathbb{F}_q$ con $n > 2$ ha uno zero distinto da quello banale.*

## 2.2 Il simbolo di Legendre

**Definizione 2.1.** *Sia $p \neq 2$ e $\mathbb{F}_p$ il campo con $p$ elementi. Sia $x \in (\mathbb{F}_p)^*$. Si definisce il simbolo di Legendre di $x$ rispetto a $p$ , $\left(\frac{x}{p}\right)$, l'intero $x^{\frac{p-1}{2}} = \pm 1$. Il simbolo di Legendre si estende ad $\mathbb{F}_p$ ponendo $\left(\frac{0}{p}\right) = 0$.*

Per il Lemma 1.8 vale

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{se } x \text{ è un quadrato in } (\mathbb{F}_p)^* \\ -1 & \text{altrimenti} \end{cases}$$

Inoltre vale: $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$.

**Osservazione 2.1.** *Sia $x \in \mathbb{Z}$, indicheremo con $\left(\frac{x}{p}\right) = \left(\frac{\bar{x}}{p}\right)$ dove $\bar{x}$ è la riduzione modulo $p$ di $x$. Analogamente per $x \in \mathbb{Z}_p$ scriveremo $\left(\frac{x}{p}\right)$ per indicare il simbolo di Legendre di $x \mod p$ rispetto a $p$.*

**Definizione 2.2.** *Sia $n$ un intero dispari. Si definiscono le funzioni $\epsilon(n)$ e $\omega(n)$ a valori in $\mathbb{Z}/2\mathbb{Z}$ ponendo:*

$$\epsilon(n) = \frac{n-1}{2} \pmod 2 = \begin{cases} 0 & \text{se } n = 1 \mod 4 \\ 1 & \text{se } n = -1 \mod 4 \end{cases}$$

*e*

$$\omega(n) = \frac{n^2-1}{8} \pmod 2 = \begin{cases} 0 & \text{se } n = \pm 1 \mod 8 \\ 1 & \text{se } n = \pm 5 \mod 8 \end{cases}$$

**Osservazione 2.2.** *La funzione $\epsilon(n)$ è un omomorfismo del gruppo moltiplicativo $(\mathbb{Z}/4\mathbb{Z})^*$ in $\mathbb{Z}/2\mathbb{Z}$ e, in particolare, vale che $\epsilon(nm) = \epsilon(n) + \epsilon(m)$. Analogamente $\omega(n)$ è un omomorfismo del gruppo moltiplicativo $(\mathbb{Z}/8\mathbb{Z})^*$ in $\mathbb{Z}/2\mathbb{Z}$ e, in particolare, si ha $\omega(nm) = \omega(n) + \omega(m)$.*

Infatti siano $n$ ed $m$ due interi dispari, allora $n, m = \pm 1 \mod 4$. Se $n = m = 1 \mod 4$ allora anche $nm = 1 \mod 4$ e $\epsilon(nm) = 0 = \epsilon(n) + \epsilon(m)$. Se $n = 1 \mod 4$ e $m = -1 \mod 4$ e quindi $nm = -1 \mod 4$, si ha che $\epsilon(nm) = 1 = 0 + 1 = \epsilon(n) + \epsilon(m)$. Infine se $n = m = -1 \mod 4$ allora $nm = 1 \mod 4$ e $\epsilon(nm) = 0 = 1 + 1 = \epsilon(n) + \epsilon(m)$. Allo stesso modo se $n = m = \pm 1 \mod 8$ oppure $n = 1 \mod 8$ ed $n = -1 \mod 8$, si ha $nm = \pm 1 \mod 8$ e $\epsilon(nm) = 0 = 0 + 0 = \epsilon(n) + \epsilon(m)$. Se $n = \pm 1 \mod 8$ e $m = \pm 5 \mod 8$ allora $nm = \pm 5 \mod 8$ e $\epsilon(nm) = 1 = 0 + 1 = \epsilon(n) + \epsilon(m)$. Infine se $n = m = \pm 5 \mod 8$ oppure $n = 5 \mod 8$ e $m = -5 \mod 8$, si ha che $nm = \pm 1 \mod 8$ e $\epsilon(nm) = 0 = 1 + 1 = \epsilon(n) + \epsilon(m)$.

**Proposizione 2.1.** *Sia $p$ un primo dispari. Allora*

1. $\left(\frac{1}{p}\right) = 1$
2. $\left(\frac{-1}{p}\right) = (-1)^{\epsilon(p)}$
3. $\left(\frac{2}{p}\right) = (-1)^{\omega(p)}$

*Dimostrazione.* Chiaramente 1 è un quadrato in $\mathbb{F}_p$ e $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ quindi la 1. e la 2. seguono facilmente dalla Definizione 2.1. Mostriamo la 3. Sia $\Omega$ una opportuna estensione del campo $\mathbb{F}_p$ e $\alpha \in \Omega$ radice primitiva ottava dell'unità. Pongo $y = \alpha + \alpha^{-1}$. Allora $y^2 = (\alpha^2 + \alpha^{-2} + 2) = \alpha^{-2}(\alpha^4 + 1) + 2 = 2$, cioè $y$ è radice di 2. Ora $\left(\frac{2}{p}\right) = 1$ se e solo se $y \in \mathbb{F}_p$ se e solo se $y^{p-1} = 1$. Se $p = \pm 1 \mod 8$, $y^p = y$ e $\left(\frac{2}{p}\right) = y^{p-1} = 1$. Se invece $p = \pm 5 \mod 8$, si ha $y^p = \alpha^p + \alpha^{-p} = \alpha^5 + \alpha^{-5} = -\alpha - \alpha^{-1} = -y$ (ricordo che $\alpha$ è radice di $X^4 + 1$). Ma allora $y^{p-1} = -1$ e dunque $\left(\frac{2}{p}\right) = -1$. □

**Teorema 2.2** (Legge di reciprocità quadratica)**.** *Siano $p$ ed $l$ due primi dispari. Allora*

$$\left(\frac{p}{l}\right) = (-1)^{\epsilon(p)\epsilon(l)} \left(\frac{l}{p}\right)$$

*Dimostrazione.* Sia $\Omega$ una opportuna estensione di $\mathbb{F}_p$ e $\omega \in \Omega$ una radice primitiva $l$-esima dell'unità. Definisco $y \in \Omega$ come la somma di Gauss nel modo seguente:

$$y = \sum_{x \in \mathbb{F}_l} \omega^x \left(\frac{x}{l}\right)$$

Allora valgono:

1. $y^2 = (-1)^{\epsilon(l)} l$
2. $y^{p-1} = \left(\frac{p}{l}\right)$

Infatti per la prima:

$$y^2 = \sum_{x,z \in \mathbb{F}_l} \omega^{x+z} \left(\frac{x}{l}\right)\left(\frac{z}{l}\right) = \sum_{x,z \in \mathbb{F}_l} \omega^{x+z} \left(\frac{xz}{l}\right) = \sum_{t \in \mathbb{F}_l} \omega^t \sum_{z \in (\mathbb{F}_l)^*} \left(\frac{z(t-z)}{l}\right)$$

Se $t = 0$

$$\sum_{z\in(\mathbb{F}_l)^*}\left(\frac{z(t-z)}{l}\right) = \sum_{z\in(\mathbb{F}_l)^*}\left(\frac{-z^2}{l}\right) = \sum_{z\in(\mathbb{F}_l)^*}\left(\frac{-1}{l}\right) = (l-1)(-1)^{\epsilon(l)}$$

Sia $t \neq 0$ allora se $z \neq 0$ si ha che $\left(\frac{z(t-z)}{l}\right) = \left(\frac{-z^2(-tz^{-1}+1)}{l}\right) = \left(\frac{-z^2}{l}\right)\left(\frac{(-tz^{-1}+1)}{l}\right)$. Ne consegue che

$$\sum_{z\in(\mathbb{F}_l)^*}\left(\frac{z(t-z)}{l}\right) = \sum_{z\in(\mathbb{F}_l)^*}\left(\frac{-1}{l}\right)\left(\frac{1-tz^{-1}}{l}\right) = (-1)^{\epsilon(l)}\sum_{w\in(\mathbb{F}_l)^*\setminus\{1\}}\left(\frac{w}{l}\right)$$

E inoltre

$$\sum_{w\in(\mathbb{F}_l)^*\setminus\{1\}}\left(\frac{w}{l}\right) = \sum_{w\in(\mathbb{F}_l)^*}\left(\frac{w}{l}\right) - 1$$

I quadrati in $(\mathbb{F}_l)^*$ formano un sottogruppo di indice due, dunque in $(\mathbb{F}_l)^*$ vi sono un egual numero di quadrati e non quadrati, cioè $\sum_{w\in(\mathbb{F}_l)^*}\left(\frac{w}{l}\right) = 0$. Otteniamo infine:

$$\begin{aligned} y^2 &= \sum_{t\in\mathbb{F}_l}\omega^t\sum_{z\in(\mathbb{F}_l)^*}\left(\frac{z(t-z)}{l}\right) = (l-1)(-1)^{\epsilon(l)} + \sum_{t\in(\mathbb{F}_l)^*}\omega^t(-1)^{\epsilon(l)}(-1) \\ &= (-1)^{\epsilon(l)}\left(l-1-\sum_{t\in(\mathbb{F}_l)^*}\omega^t\right) = (-1)^{\epsilon(l)}l \end{aligned}$$

Dove abbiamo usato il fatto che il $l$-esimo polinomio ciclotomico è $X^{l-1}+X^{l-2}+...+X+1$ e dunque $\omega^{l-1}+\omega^{l-2}+...+\omega = -1$.
Per la seconda, ricordando che $x \longrightarrow x^p$ è un omomorfismo in un campo di caratteristica $p$, ho:

$$y^p = \sum_{x\in\mathbb{F}_l}\omega^{xp}\left(\frac{x}{l}\right) = \sum_{z\in\mathbb{F}_l}\omega^z\left(\frac{zp^{-1}}{l}\right) = \sum_{z\in\mathbb{F}_l}\omega^z\left(\frac{z}{l}\right)\left(\frac{p}{l}\right) = \left(\frac{p}{l}\right)\sum_{z\in\mathbb{F}_l}\omega^z\left(\frac{z}{l}\right) = \left(\frac{p}{l}\right)y$$

Cioè $y^{p-1} = \left(\frac{p}{l}\right)$. Ora possiamo concludere facilmente grazie alla 1. e alla 2.

$$\left(\frac{p}{l}\right) = y^{p-1} = \left(\frac{y^2}{p}\right) = \left(\frac{(-1)^{\epsilon(l)}l}{p}\right) = \left(\frac{(-1)^{\epsilon(l)}}{p}\right)\left(\frac{l}{p}\right) = (-1)^{\epsilon(p)\epsilon(l)}\left(\frac{l}{p}\right)$$

□

## 2.3 Il simbolo di Hilbert

In questa sezione indicheremo con $K$ il campo dei reali $\mathbb{R}$ e i campi dei numeri $p$-adici $\mathbb{Q}_p$ per ogni primo $p$.

**Definizione 2.3.** *Siano $a, b \in K^*$. Poniamo:*

$$(a,b) = \begin{cases} 1 & \text{se l'equazione } Z^2 - aX^2 - bY^2 = 0 \text{ ha una soluzione in } K^3 \setminus \{(0,0,0)\} \\ -1 & \text{altrimenti} \end{cases}$$

*$(a,b)$ è detto simbolo di Hilbert di $a$ e $b$.*

**Osservazione 2.3.** *Il simbolo di Hilbert $(a,b)$ non cambia se $a$ e $b$ sono moltiplicati da quadrati, dunque definisce una mappa $(\cdot\ ,\ \cdot) : K^*/K^{*2} \times K^*/K^{*2} \longrightarrow \{\pm 1\}$*

Preso $b \in K^*$, sia $\beta$ una radice quadrata di $b$ in una opportuna estensione del campo $K$. Indichiamo $K_b = K(\beta)$ e $NK_b^*$ il gruppo delle norme in $K_b^*$.

**Proposizione 2.2.** *Siano $a, b \in K^*$. Il simbolo di Hilbert $(a,b) = 1$ se e solo se $a \in NK_b^*$.*

*Dimostrazione.* Sia $b$ un quadrato in $K^*$. Allora $b = c^2$ per un certo $c \in K^*$. Ne consegue che l'equazione $Z^2 - aX^2 - bY^2 = 0$ ha soluzione non banale $(c, 0, 1)$, cioè $(a,b) = 1$ e $K = K_b$, quindi l'enunciato è banalmente verificato. Sia ora $\beta$ una radice di $b$. Un elemento in $K_b$ è $\eta = z + \beta y$ al variare di $z, y \in K$ e la sua norma è $N(\eta) = z^2 - by^2$. Se $a \in NK_b^*$ allora $a = z^2 - by^2$ e l'equazione $Z^2 - aX^2 - bY^2 = 0$ ha soluzione $(z, 1, y) \neq (0,0,0)$. Viceversa se esiste una soluzione $(x, y, z)$ non banale all'equazione $Z^2 - aX^2 - bY^2 = 0$, possiamo supporre $x \neq 0$ (altrimenti siamo nel caso $K = K_b$) e allora $z^2 - ax^2 - by^2 = 0$, cioè $a = \frac{z^2}{x^2} - \frac{by^2}{x^2}$. □

**Proposizione 2.3.** *Il simbolo di Hilbert verifica le seguenti proprietà:*

1. $(a,b) = (b,a)$ *e* $(a, c^2) = 1$
2. $(a, -a) = 1$ *e* $(a, 1-a) = 1$
3. *Se* $(a,b) = 1$ *allora* $(ac, b) = (c, b)$
4. $(a,b) = (a, -ab)$ *e* $(a,b) = (a, b(1-a))$

*Dimostrazione.* Il simbolo di Hilbert è evidentemente simmetrico e inoltre l'equazione $Z^2 - aX^2 - c^2y^2 = 0$ ha soluzione $(c, 0, 1)$. D'altro lato $Z^2 - aX^2 + aY^2$ e $Z^2 - aX^2 - (1-a)Y^2$ hanno soluzioni rispettivamente $(0, 1, 1)$ e $(1, 1, 1)$. Ciò mostra la 1. e la 2. Per la 3. osserviamo che $(a,b) = 1$ implica che $a \in NK_b^*$ per la Proposizione 2.2. Ma allora $(ac, b) = 1$ se e solo se $ac \in NK_b^*$ se e solo se $c \in NK_b^*$ se e solo se $(c,b) = 1$. Infine la 4. segue banalmente dai punti precedenti. □

Enunciamo il seguente lemma:

**Lemma 2.2.** *Sia $p$ primo e $u \in (\mathbb{Z}_p)^*$. Se l'equazione $Z^2 - pX^2 - uY^2 = 0$ ammette una soluzione non banale in $\mathbb{Q}_p^3$, allora essa amette una soluzione primitiva $(z, x, y)$ in $\mathbb{Z}_p^3$ tale che $z, y \in \mathbb{Z}_p^*$ e $x \in \mathbb{Z}_p$.*

*Dimostrazione.* Per il Lemma 1.3 l'equazione di cui sopra ammette una soluzione primitiva $(z, x, y)$ in $\mathbb{Z}_p^3$. Tale soluzione ha le proprietà richieste, infatti: se per assurdo uno tra $z$ e $y$ non appartenesse a $\mathbb{Z}_p^*$, supponiamo $y$, si avrebbe che $y = 0 \mod p$. Ma allora, riducendo modulo $p$ l'equazione, si ha che anche $z = 0 \mod p$, quindi $z \notin \mathbb{Z}_p^*$. Ne segue che $px^2 = uy^2 - z^2 = 0 \mod p^2$ e quindi $x^2 = 0 \mod p$ cioè $x = 0 \mod p$. Ma allora $x, y, z \notin \mathbb{Z}_p^*$, il che contraddice che la soluzione è primitiva. □

**Teorema 2.3** (Il calcolo del simbolo di Hilbert)**.** *Sia $K = \mathbb{R}$, $a, b \in K^*$. Allora:*

$$(a,b) = \begin{cases} 1 & \text{se almeno uno tra } a \text{ e } b \text{ è strettamente positivo} \\ -1 & \text{altrimenti} \end{cases}$$

*Sia $K = \mathbb{Q}_p$ e $a = p^\alpha u$, $b = p^\beta v$ dove $\alpha, \beta \in \mathbb{Z}$ e $u, v \in (\mathbb{Z}_p)^*$. Se $p \neq 2$:*

$$(a,b) = (-1)^{\epsilon(p)\alpha\beta} \left(\frac{v}{p}\right)^\alpha \left(\frac{u}{p}\right)^\beta$$

*Se $p = 2$:*

$$(a,b) = (-1)^{\epsilon(u)\epsilon(v)+\alpha\omega(v)+\beta\omega(u)}$$

*Dimostrazione.* Il caso $K = \mathbb{R}$ è banale. Mostriamo il teorema per $p \neq 2$. Si noti che, presi $a = p^\alpha u$ e $b = p^\beta v$ in $\mathbb{Q}_p$, il contributo degli esponenti $\alpha$ e $\beta$ nella formula del teorema è dato dalla loro riduzione modulo due, quindi basta considerare i casi seguenti:

1. $\alpha = 0$ e $\beta = 0$. Dobbiamo mostrare che $(u, v) = 1$, cioè che la forma quadratica $f(Z, X, Y) = Z^2 - uX^2 - vY^2$ ha uno zero non banale. Tuttavia $f \mod p$ è una forma quadratica in tre variabili sul campo $\mathbb{F}_p$ e per il Corollario 2.2 ammette uno zero non banale. Tale soluzione può essere sollevata ad una vera soluzione in $\mathbb{Z}_p^3$ per il Corollario 1.1, il che permette di concludere che $(u, v) = 1$.

2. $\alpha = 1$ e $\beta = 0$. Dobbiamo mostrare che $(pu, v) = \left(\frac{v}{p}\right)$. Dalla Proposizione 2.3 e dal punto precedente si ha che $(pu, v) = (p, v)$, quindi la tesi è equivalente a $(p, v) = \left(\frac{v}{p}\right)$. Se $v$ è un quadrato in $\mathbb{Z}_p^*$ allora $(p, v) = 1$ per la Proposizione 2.3 e la riduzione modulo $p$ di $v$ è un quadrato in $\mathbb{F}_p^*$ quindi $\left(\frac{v}{p}\right) = 1$. Invece se $v$ non è un quadrato e $\left(\frac{v}{p}\right) = -1$, sia per assurdo $(p, v) = 1$, cioè l'equazione $Z^2 - pX^2 - vY^2 = 0$ ammette una soluzione non banale in $\mathbb{Q}_p^3$. Per il Lemma 2.2 esiste una soluzione $(z, x, y)$ con $z, y \in \mathbb{Z}_p^*$ e $x \in \mathbb{Z}_p$. Allora $z^2 - px^2 - vy^2 = 0 \mod p$ se e solo se $z^2 - vy^2 = 0 \mod p$ se e solo se $v = z^2 y^{-2} \mod p = (zy^{-1})^2 \mod p$ cioè $v$ è un quadrato $\pmod p$ dunque $v$ è un quadrato in $\mathbb{Z}_p^*$ e questa è una contraddizione.

3. $\alpha = 1$ e $\beta = 1$. L'ultimo caso equivale a mostrare che $(pu, pv) = (-1)^{\epsilon(p)} \left(\frac{u}{p}\right)\left(\frac{v}{p}\right)$. Per la Proposizione 2.3 vale $(pu, pv) = (pu, -p^2uv) = (pu, -uv)$. Dal punto precedento ho: $(pu, -uv) = \left(\frac{-uv}{p}\right)$. Per le proprietà del simbolo di Legendre

$$(pu, pv) = (pu, -uv) = \left(\frac{-uv}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{u}{p}\right)\left(\frac{v}{p}\right) = (-1)^{\epsilon(p)} \left(\frac{u}{p}\right)\left(\frac{v}{p}\right)$$

Il che conclude il caso $p \neq 2$. Vogliamo ora dimostrare il teorema per $p = 2$. Siano $a = 2^\alpha u$ e $b = 2^\beta v$ con $u, v \in \mathbb{Z}_2^*$. Come sopra osserviamo che gli esponenti $\alpha$ e $\beta$ contribuiscono alla formula tramite la loro riduzione (mod 2), quindi ancora una volta distinguiamo i casi:

1. $\alpha = 0$ e $\beta = 0$. Dobbiamo mostrare che $(u, v) = (-1)^{\epsilon(u)\epsilon(v)}$ cioè $(u, v) = 1$ se almeno un tra $u$ e $v$ è congruo a $1 \mod 4$ e $(u, v) = -1$ altrimenti. Sia $v = 1 \mod 4$. Allora $v = 1 \mod 8$ oppure $v = 5 \mod 8$. Nel primo caso $v$ è un quadrato in $\mathbb{Z}_2^*$ per la Proposizione 1.9 e per la Proposizione 2.3 $(u, v) = 1$. Nel secondo

caso, considero $v+4u$. Si noti che $v+4u = 1 \mod 8$ ed è un quadrato in $\mathbb{Z}_2^*$. Sia $w \in \mathbb{Z}_2^*$ tale che $w^2 = v+4u$, allora l'equazione $Z^2 - uX^2 - vY^2$ ha soluzione $(w,1,2) \neq (0,0,0)$. D'altro lato siano $u, v = -1 \mod 4$. Se fosse $(u,v) = 1$ allora l'equazione $Z^2 - uX^2 - vY^2$ ha una soluzione primitiva $(z,x,y) \in \mathbb{Z}_p^3$ per il Lemma 1.3. Quindi $z^2 - ux^2 - vy^2 = z^2 + x^2 + y^2 \mod 4$ e $z^2+x^2+y^2 = 0 \mod 4$. Tuttavia gli unici quadrati in $\mathbb{Z}/4\mathbb{Z}$ sono 0 e 1, quindi necessariamente $z^2 = x^2 = y^2 = 0 \mod 4$ e anche $z = x = y = 0 \mod 2$, il che contraddice che la soluzione è primitiva.

2. $\alpha = 1$ e $\beta = 0$. Equivale a mostrare che $(2u,v) = (-1)^{\epsilon(u)\epsilon(v)+\omega(v)}$. Cominciamo ad osservare che $(2,v) = (-1)^{\omega(v)}$ cioè $(2,v) = 1$ se e solo se $v = \pm 1 \mod 8$. Infatti se $v = 1 \mod 8$ allora $v$ è un quadrato in $\mathbb{Z}_2^*$ e per la Proposizione 2.3 $(2,v) = 1$. Sia $v = -1 \mod 8$ e consideriamo l'equazione $f(Z,X,Y) = Z^2 - 2X^2 - vY^2 = Z^2 - 2X^2 + Y^2 \mod 8$. Essa ha soluzione $(1,1,1)$ che verifica le ipotesi del Corollario 1.2 e dunque si solleva ad una soluzione di $f$ in $\mathbb{Z}_2$. Viceversa sia $(2,v) = 1$ e $(z,x,y)$ una soluzione dell'equazione $f = 0$ come nel Lemma 2.2, cioè $z, y \in \mathbb{Z}_2^*$ e $x \in \mathbb{Z}_2$. Allora $z^2 - 2x^2 - vy^2 = 0 \mod 8$. Gli unici quadrati (mod 8) sono 0,1 e 4 e necessariamente $z^2, y^2 = 1 \mod 8$ altrimenti si avrebbe $z, y \in 2\mathbb{Z}_2$. Dunque $1 - 2x^2 - v = 0 \mod 8$ che implica che: $1 - v = 0 \mod 8$ ovvero $v = 1 \mod 8$, se $x^2 = 0 \mod 8$ o $x^2 = 4 \mod 8$, e $1 - 2 - v = 0 \mod 8$ cioè $v = -1 \mod 8$, se $x^2 = 1 \mod 8$.
   Per concludere basta mostrare che $(2u,v) = (u,v)(2,v)$. Chiaramente se $(u,v) = 1$ oppure $(2,v) = 1$ la tesi è vera per la Proposizione 2.3. Siano ora $(u,v) = -1$ e $(2,v) = -1$, mostro che $(2u,v) = 1$. Considero l'equazione $Z^2 - 2uX^2 - vY^2 = 0$. Da $(2,v) = -1$ segue, per quanto osservato prima, che $v = \pm 5 \mod 8$ e da $(u,v) = -1$ segue, per il punto 1, che $u = -1 \mod 4$ e $v = -1 \mod 4$. Allora necessariamente $v = 3 \mod 8$ e $u = -1 \mod 8$ opppure $u = 3 \mod 8$. Nel primo caso, riducendo (mod 8) l'equazione di cui sopra, si ha $Z^2 + 2X^2 - 3Y^2 = 0 \mod 8$ e nel secondo $Z^2 - 6X^2 - 3Y^2 = 0 \mod 8$. Le due forme quadratiche hanno zero $(1,1,1)$ modulo 8, che per il Corollario 1.2 si solleva ad una soluzione in $\mathbb{Z}_2^3$. Ciò mostra che vale

$$(2u,v) = (u,v)(2,v) = (-1)^{\epsilon(u)\epsilon(v)}(-1)^{\omega(v)} = (-1)^{\epsilon(u)\epsilon(v)+\omega(v)}$$

   Il che conclude il caso 2.

3. $\alpha = 1$ e $\beta = 1$. Dobbiamo mostrare che $(2u,2v) = (-1)^{\epsilon(u)\epsilon(v)+\omega(v)+\omega(u)}$. Per la Proposizione 2.3 si ha $(2u,2v) = (2u,-4uv) = (2u,-uv)$ e per il punto precedente $(2u,-uv) = (-1)^{\epsilon(u)\epsilon(-uv)+\omega(-uv)}$. Ricordando che $\epsilon$ e $\omega$ sono omomorfismi, si ha:

$$\epsilon(u)\epsilon(-uv) = \epsilon(u)(\epsilon(-1) + \epsilon(u) + \epsilon(v)) = \epsilon(u)(1+\epsilon(u)) + \epsilon(u)\epsilon(v) = \epsilon(u)\epsilon(v)$$

   poichè $\epsilon(u)(1+\epsilon(u)) = 0$. E anche

$$\omega(-uv) = \omega(-1) + \omega(u) + \omega(v) = \omega(u) + \omega(v)$$

   Il che permette di concludere.

□

**Corollario 2.3.** *Sia $K = \mathbb{Q}_p$. Il simbolo di Hilbert verifica le seguenti proprietà*

1. $(ac, b) = (a, b)(c, b)$ *per ogni* $a, b, c \in K^*$.
2. *Per ogni* $b \in K^*$ *si ha* $(a, b) = 1$ *per ogni* $a \in K^*$ *se e solo se* $b \in K^{*2}$.

*Dimostrazione.* La proprietà 1. segue immediatamente dalle formule del calcolo del simbolo di Hilbert nei casi $p \neq 2$ e $p = 2$. Per mostrare la 2. basta trovare per ogni $x \in K^*$ che non sia un quadrato un elemento $y$ tale che $(x, y) = -1$. Sia $p \neq 2$. Sappiamo dalla Proposizione 1.8 che $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ e che $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} = \{u, p, pu, 1\}$ dove $u \in \mathbb{Z}_p^*$ non è un quadrato. Ma allora dal Teorema precedente si evince che $(u, p) = (p, u) = -1$ e $(pu, u) = (p, u)(u, u) = -1$. Sia ora $p = 2$. Sappiamo dalla proposizione 1.9 che $x = 2^\alpha u$ in $\mathbb{Q}_2$, è un quadrato se e solo se $\alpha = 0 \mod 2$ e $u = 1 \mod 8$, dunque $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ è descritto da $\{u, 2u\}$ dove $u \in \{\pm 1, \pm 5\} \pmod 8$ non è un quadrato in $\mathbb{Z}_2^*$. Dal Teorema 2.3 abbiamo $(5, 2u) = -1$ e $(-1, -1) = (-5, -5) = -1$. □

## 2.4 Il teorema di Hilbert

Sia $V$ l'insieme $V = \{p \in \mathbb{Z} \text{ tale che } p \text{ è primo}\} \cup \{\infty\}$. Siano $a, b \in \mathbb{Q}^*$, indicheremo con $(a, b)_v$ il simbolo di Hilbert di $a, b \in \mathbb{Q}_v$ per ogni $v \in V$ con $v$ primo e con $(a, b)_\infty$ il simbolo di Hilbert di $a$ e $b$ in $\mathbb{R}$.

**Teorema 2.4** (Hilbert)**.** *Siano $a$ e $b$ in $\mathbb{Q}^*$. Allora $(a, b)_v = 1$ per quasi ogni $v \in V$ e*

$$\prod_{v \in V} (a, b)_v = 1$$

*Dimostrazione.* Per il Corollario 2.3 basta mostrare il teorema per $a$ e $b$ primi o uguali a $-1$ e il caso generale segue per le proprietà di $(\cdot, \cdot)$.

1. Siano $a = b = -1$. Allora $(-1, -1)_\infty = (-1, -1)_2 = -1$ e $(-1, -1)_v = 1$ per ogni $v \neq 2$ per il Teorema 2.3. Ne consegue che $(-1, -1) = 1$ per ogni $v \in V \setminus \{2, \infty\}$ e il prodotto $\prod_{v \in V} (-1, -1)_v = 1$.
2. Siano $a = p$ e $b = -1$ con $p$ primo. Sia $p = 2$, allora $(2, -1)_v = 1$ se $v \neq 2$ e $(2, -1)_2 = 1$ dunque $(2, -1)_v = 1$ per ogni $v \in V$ e il prodotto di cui sopra è uguale ad 1. Sia $p \neq 2$, allora $(p, -1)_v = 1$ se $v \neq p$ e $v \neq 2$ e $(p, -1)_p = \left(\frac{-1}{p}\right) = (-1)^{\epsilon(p)}$ e $(p, -1)_2 = (-1)^{\epsilon(p)}$. Ne consegue che $\prod_{v \in V} (p, -1)_v = (-1)^{\epsilon(p)}(-1)^{\epsilon(p)} = 1$.
3. Siano $a = p$ e $b = l$ primi distinti. Se $p = 2$ vale che $(2, l)_v = 1$ se $v \neq l, 2$ e $(2, l)_l = \left(\frac{2}{l}\right) = (-1)^{\omega(l)}$ per la Proposizione 2.1 e $(2, l)_2 = (-1)^{\omega(l)}$. Dunque $\prod_{v \in V} (p, l)_v = (-1)^{\omega(l)}(-1)^{\omega(l)} = 1$ e il teorema è verificato. Infine siano $p, l \neq 2$. Allora $(p, l)_2 = (-1)^{\epsilon(l)\epsilon(p)}$ e $(p, l)_v = 1$ se $v \neq l, p$. D'altra parte $(p, l)_p = \left(\frac{l}{p}\right)$ e $(p, l)_l = \left(\frac{p}{l}\right)$. Infine

$$\prod_{v \in V} (p, l)_v = (-1)^{\epsilon(l)\epsilon(p)} \left(\frac{l}{p}\right) \left(\frac{p}{l}\right) = \left(\frac{l}{p}\right) \left(\frac{l}{p}\right) = 1$$

Dove ho usato la legge di reciprocità quadratica $\left(\frac{l}{p}\right) = (-1)^{\epsilon(l)\epsilon(p)} \left(\frac{p}{l}\right)$.

□

## 2.5 Razionali con simboli di Hilbert assegnati

Enunciamo ora un importante risultato.

**Teorema 2.5.** *Sia $(a_i)_i \in I$ una famiglia finita di razionali e $\varepsilon_{i,v}$ per $i \in I$ e $v \in V$ una successione di valori in $\{\pm 1\}$. Esiste un $x \in \mathbb{Q}^*$ tale che $(x, a_i)_v = \varepsilon_{i,v}$ per ogni $i \in I$ e $v \in V$ se e solo se*

1. *$\varepsilon_{i,v} = 1$ per quasi ogni $i \in I$, $v \in V$*
2. *Per ogni $i \in I$ si ha $\prod_{v \in V} \varepsilon_{i,v} = 1$*
3. *Per ogni $v \in V$ esiste un $x_v \in \mathbb{Q}_v$ tale che $(x_v, a_i)_v = \varepsilon_{i,v}$ per ogni $i \in I$*

*Dimostrazione.* La necessità dei punti 1. e 2. deriva dal Teorema 2.4, mentre per il punto 3. basta prendere $x_v = x$ per ogni $v$. Per mostrare la sufficienza è opportuno enunciare dei lemmi preliminari.

**Lemma 2.3** (Teorema cinese del resto)**.** *Siano $a_1, a_2, ..., a_n \in \mathbb{Z}$ e $m_1, m_2, ..., m_n$ degli interi a due a due coprimi. Allora esiste un $a \in \mathbb{Z}$ tale che $a = a_k \mod m_k$ per ogni $k = 1, 2, ..., n$.*

*Dimostrazione.* Sia $m = m_1 m_2 ... m_n$ e si consideri l'applicazione

$$\Phi : \mathbb{Z}/m\mathbb{Z} \longrightarrow \prod_{k=1}^{n} \mathbb{Z}/m_k\mathbb{Z}$$

definita ponendo $\Phi(x) = (x \mod m_1,\ x \mod m_2, ...,\ x \mod m_n)$. Chiaramente è ben definita: se $x = x' \mod m$ allora $m$ divide $x - x'$ ma $m = m_1 m_2 ... m_n$ dunque $m_i$ divide $x - x'$ $\forall i$ cioè $x = x' \mod m_i$. Se mostro che è una biiezione ho concluso. Tale funzione è iniettiva. Siano infatti $x$ e $x' \in \mathbb{Z}/m\mathbb{Z}$ tali che $x = x' \mod m_i$ per $i = 1, 2..., n$ allora $m_i$ divide $x - x'$ per ogni $i$, allora il minimo comune multiplo degli $m_i$ divide la differenza $x - x'$. Ma gli $m_i$ sono coprimi quindi $m = m_1 m_2 ... m_n$ divide $x - x'$, cioè $x = x' \mod m$. D'altro lato gli anelli $\mathbb{Z}/m\mathbb{Z}$ e $\prod_{k=1}^{n} \mathbb{Z}/m_k\mathbb{Z}$ hanno la stessa cardinalità finita, dunque $\Phi$ è anche suriettiva, il che permette di concludere. □

**Lemma 2.4** (Teorema di approssimazione)**.** *Sia $S \subseteq V$ un sottoinsieme finito. Allora $\mathbb{Q}$ è denso in $\prod_{v \in S} \mathbb{Q}_v$.*

*Dimostrazione.* Non è restrittivo supporre che $S = \{p_1, p_2, ..., p_n, \infty\}$. Sia dato un elemento $(x_1, x_2, ..., x_n, x_\infty)$ del prodotto $\mathbb{Q}_{p_1} \times \mathbb{Q}_{p_2} \times ... \times \mathbb{Q}_{p_n} \times \mathbb{R}$. La tesi equivale a mostrare che per ogni $\epsilon > 0$ e $N \in \mathbb{N}$, esiste un $x \in \mathbb{Q}$ tale che $|x - x_\infty| \leq \epsilon$ e $|x - x_i|_{p_i} \leq p_i^{-N}$ cioè $ord_{p_i}(x - x_i) \geq N$ per ogni $i = 1, 2, ..., n$. Applico il Lemma 2.3 con $m_i = p_i^N$ e trovo $x_0 \in \mathbb{Q}$ tale che $x_0 = x_i \mod p_i^N$ cioè $ord_{p_i}(x_0 - x_i) \geq N$. Sia ora $q$ un intero coprimo

con i $p_i$, allora i razionali del tipo $\frac{a}{q^m}$ sono densi in $\mathbb{R}$. Posso allora trovare un $m \in \mathbb{N}$ e un $a \in \mathbb{Z}$ tale che:

$$\left| x_\infty - x_0 - \frac{a}{q^m} p_1^N p_2^N ... p_n^N \right| \leq \epsilon$$

Se pongo $x = x_0 + p_1^N p_2^N ... p_n^N \frac{a}{q^m}$ ho concluso. □

**Lemma 2.5** (Teorema di Dirichlet)**.** *Siano $a$ e $b$ due interi coprimi. Esistono infiniti primi $p$ tali che $p = a \mod b$.*

*Dimostrazione.* Vedi Appendice A. □

Possiamo ora procedere alla dimostrazione del Teorema 2.5. A meno di moltiplicazione per quadrati di interi, possiamo supporre che gli $a_i$ siano interi. Sia $S$ il sottoinsieme di $V$ costituito da 2,$\infty$ e dai fattori primi degli $a_i$. Sia inoltre $T$ l'insieme dei $v \in V$ tali che esiste un $i \in I$ che verifica $\varepsilon_{i,v} = -1$. Distinguiamo due casi:

*i)* $S \cap T = \emptyset$. Pongo

$$a = \prod_{l \in T,\ l \neq \infty} l \quad \text{e} \quad b = 8 \prod_{l \in S,\ l \neq 2,\infty} l$$

Poiché i sottoinsiemi $S$ e $T$ hanno intersezione vuota, $a$ e $b$ sono coprimi. Per il Lemma 2.5 esiste un primo $p$ tale che $p \notin S \cup T$ e $p = a \mod b$. L'intero $x = pa$ è il razionale cercato: mostriamolo. Se $v \in S$, poichè $S \cap T = \emptyset$, ho che $(a_i, x)_v = \varepsilon_{i,v} = 1$ per ogni $i \in I$, allora devo mostare che $(a_i, pa)_v = 1$. Se $v = \infty$, poiché $x > 0$, dal Teorema 2.3 ho $(a_i, x)_\infty = 1\ \forall i \in I$. Sia ora $l \neq \infty$ e $x = ap = a^2 \mod b$. Allora $x = a^2 \mod l$ per ogni $l \neq 2$ in $S$ e $x = a^2 \mod 8$. Inoltre $a$ e $x$ sono coprimi con $l$ per $l \in S$, allora sono invertibili in $\mathbb{Z}_l$. Per la Proposizione 1.8 e 1.9, $x$ è un quadrato in $\mathbb{Q}_l$, dunque $(a_i, x)_l = (a_i, x)_2 = 1$ per le proprietà del simbolo di Hilbert. Se invece $l \notin S$, $l$ non divide $a_i$ e quindi $a_i$ è invertibile in $\mathbb{Z}_l$. Allora per il Teorema 2.3

$$(a_i, x)_l = \left(\frac{a_i}{l}\right)^{ord_l(x)}$$

Se $l \notin T \cup \{p\}$, per ipotesi $\varepsilon_{i,l} = 1$ per ogni $i \in I$. Quindi ancora una volta dobbiamo mostrare che $(a_i, x)_l = 1$. Ma $x = ap$ e $l$ non divide $x$ quindi $ord_l(x) = 0$, dunque $\left(\frac{a_i}{l}\right)^{ord_l(x)} = 1 = (a_i, x)_l$. Se invece $l \in T$, $ord_l(x) = 1$ e quindi $(a_i, x)_l = \left(\frac{a_i}{l}\right)$. Inoltre per ipotesi esiste un $x_l \in \mathbb{Q}_l^*$ tale che $(a_i, x_l)_l = \varepsilon_{i,l}$ con $(a_i, x_l)_l = \left(\frac{a_i}{l}\right)^{ord_l(x_l)}$. Si noti che, poiché $l \in T$ esiste $i$ tale che $\varepsilon_{i,l} = -1$, deve necessariamente essere $ord_l(x_l) = 1 \mod 2$ e quindi

$$(a_i, x)_l = \left(\frac{a_i}{l}\right) = (a_i, x_l)_l = \varepsilon_{i,l} \quad \forall i \in I$$

Infine se $l = p$, per i Teorema di Hilbert abbiamo che il prodotto su $v \in V$ degli $(a_i, x)_v$ è uguale ad 1 per ogni $i$ e per ipotesi anche $\prod_{v \in V} \varepsilon_{i,v}$ per ogni $i$. Ciò basta per concludere che

$$(a_i, x)_p = \prod_{v \in V, v \neq p} (a_i, x)_v = \prod_{v \in V, v \neq p} \varepsilon_{i,v} = \varepsilon_{i,p} \ \ \forall i \in I$$

*ii*) Sia l'intersezione tra $S$ e $T$ non necessariamente vuota. La Proposizione 1.8 e 1.9 ci dicono che il sottogruppo $\mathbb{Q}_p^{*2}$ di $\mathbb{Q}_p^*$ è un aperto. Per il Lemma 2.4 esiste un $x' \in \mathbb{Q}$ tale che $\frac{x'}{x_v}$ è un quadrato in $\mathbb{Q}_v^*$ per ogni $v \in S$. Allora $(a_i, x')_v = (a_i, x_v)_v = \varepsilon_{i,v}$ per $v \in S$. Pongo $\varepsilon'_{i,v} = \varepsilon_{i,v}(a_i, x')_v$. Allora $\varepsilon'_{i,v} = 1$ per ogni $v \in S$ e la successione dei $\varepsilon'_{i,v}$ soddisfa ancora le ipotesi del teorema. Per il punto $i$) esiste un $y \in \mathbb{Q}$, tale che $(a_i, y)_v = \varepsilon'_{i,v}$ per ogni $v \in V$. Ponendo $x = x'y$ si conclude per le proprietà del simbolo di Hilbert.

□

# Capitolo 3

# Forme quadratiche

## 3.1 Forme biliniari simmetriche e moduli quadratici

Sia $K$ un campo.

**Definizione 3.1.** *Sia $V$ un $K$-spazio vettoriale. Una forma bilineare su $V$ è una mappa $\beta : V \times V \longrightarrow K$ tale che*

1. $\beta(v_1 + v_2, w) = \beta(v_1, w) + \beta(v_2, w)$
2. $\beta(v, w_1 + w_2) = \beta(v, w_1) + \beta(v, w_2)$
3. $\beta(\lambda v, w) = \lambda\beta(v, w) = \beta(v, \lambda w)$

*per ogni $v_1, v_2, w_1, w_2, v, w \in V$ e $\lambda \in K$.*

Sia ora $V$ uno spazio vettoriale di dimensione finita e $e_1, e_2, ..., e_n$ una sua base. Per ogni $i, j$ pongo $a_{ij} = \beta(e_i, e_j)$ e sia $A$ la matrice di entrate $a_{ij}$. Allora presi $x = \sum_{i=1}^{n} x_i e_i$ e $y = \sum_{j=1}^{n} = y_j e_j$

$$\beta(x, y) = \beta\left(\sum_{i=1}^{n} x_i e_i, \sum_{j=1}^{n} y_j e_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i y_j \beta(e_i, e_j) = \sum_{i,j=1}^{n} x_i y_j a_{ij} = x^t A y$$

Diremo che $A$ è la matrice associata alla forma bilineare $\beta$ nella base $e_1, e_2, ..., e_n$ di $V$. Se cambiamo base $e'_1, e'_2, ..., e'_n$ di $V$, dove $e'_i = Pe_i$ con $P$ matrice invertibile di ordine $n$ su $K$, allora siano $x' = Px$ e $y' = Py$, avremo:

$$\beta(x', y') = \beta(Px, Py) = (Px)^t A(Py) = x^t P^t A P y = x^t (P^t A P) y$$

Dunqure $\beta$ ha matrice associata nella base $e'_1, ..., e'_n$ data da $P^t AP$.

**Definizione 3.2.** *Sia $\beta : V \times V \longrightarrow K$ una forma bilineare. $\beta$ è simmetrica se $\beta(v, w) = \beta(w, v)$ per ogni $v, w \in V$.*

**Proposizione 3.1.** *Sia data una forma bilineare $\beta$ su $V$ e sia $V^*$ il duale di $V$. Definiamo:*

$$\begin{aligned} \beta_1 : V &\longrightarrow V^* & \beta_2 : V &\longrightarrow V^* \\ v &\longrightarrow \beta(v, -) : w \longrightarrow \beta(v, w) & w &\longrightarrow \beta(-, w) : v \longrightarrow \beta(v, w) \end{aligned}$$

*$\beta_1$ e $\beta_2$ sono applicazioni lineari e sono una la trasposta dell'altra.*

*Dimostrazione.* La linearità segue dalla bilinearità di $\beta$. Infine $\beta_1(v)(w) = \beta(v,w) = \beta_2(w)(v)$ e ciò mostra che sono trasposte. □

Fissiamo una base $e_1, e_2, ..., e_n$ di $V$, e consideriamo su $V^*$ la sua base duale $e_1^*, e_2^*, ..., e_n^*$. Allora $\beta_1(e_i)(e_j) = a_{ij}$, cioè $\beta_1(e_i) = a_{i1}e_1^* + .. + a_{in}e_n^*$. Dunque $\beta_1$ ha matrice nelle basi fissate $A^t$. Analogamente $\beta_2(e_i)(e_j) = a_{ji}$, ovvero $\beta_2(e_i) = a_{1i}e_1^* + ... + a_{1n}e_n^*$. La matrice di $\beta_2$ nelle basi fissate è data da $A$.

**Proposizione 3.2.** *$\beta : V \times V \longrightarrow K$ è simmetrica se e solo se $\beta_1 = \beta_2$ se e solo se $A^t = A$*

*Dimostrazione.* Segue dall'osservazione di sopra □

**Definizione 3.3.** *Sia $\beta : V \times V \longrightarrow K$ una forma bilineare su $V$. Diremo che*

1. *$\beta$ è non degenere a sinistra se $ker\beta_1 = \langle 0 \rangle$, cioè $\beta(v,w) = 0\ \forall w \in V$ implica che $v = 0$.*
2. *$\beta$ è non degenere a destra se $ker\beta_2 = \langle 0 \rangle$, cioè $\beta(v,w) = 0\ \forall v \in V$ implica che $w = 0$.*
3. *$\beta$ è non degenere se è non degenere a sinistra e a destra.*

Evidentemente vale la seguente proposizione:

**Proposizione 3.3.** *$\beta$ è non degenere se e solo se $\beta_1$ è isomorfismo se e solo se $\beta_2$ è isomorfismo se e solo se $det(A) \neq 0$.*

**Osservazione 3.1.** *Le proprietà 1. e 2. del Corollario 2.3 mostrano che il simbolo di Hilbert*

$$(\cdot,\cdot)\ :\ K^*/K^{*2} \times K^*/K^{*2} \longrightarrow \{\pm 1\}$$

*è una forma bilineare non degenere su $K^*/K^{*2}$ visto come spazio vettoriale sul campo con due elementi $\mathbb{F}_2$.*

**Definizione 3.4.** *i. Sia $V$ un $k$-spazio vettoriale. Una forma quadratica su $V$ è una funzione $q : V \to K$ tale che*

*(a) $q(\lambda v) = \lambda^2 q(v)$*

*(b) la mappa $(v,w) \longrightarrow q(v+w) - q(v) - q(w)$ è una forma bilineare simmetrica.*

*ii. Un modulo quadratico $(V,q)$ è il dato di uno spazio vettoriale $V$ e di una forma quadratica $q$ su di esso.*

**Osservazione 3.2.** *Chiaramente, data una forma bilineare simmetrica $\beta$, essa definisce una forma quadratica $q(v) = \beta(v,v)$. Ora supponiamo, fino alla fine del capitolo, che $charK \neq 2$. Data la forma quadratica $q$ su $V$, la forma bilineare simmetrica ad essa associata è data da*

$$v \cdot w = \beta_q(v,w) = \frac{1}{2}\left(q(v+w) - q(v) - q(w)\right)$$

*In particolare v'è una corrispondenza biunivoca tra forme quadratiche e forme bilineari simmetriche su $V$.*

**Osservazione 3.3.** *Diremo che $(V, q)$ è non degenere se la forma bilineare simmetrica $\beta_q$ associata a $q$ è non degenere. Diremo che $A$ è la matrice associata a $q$ nella base $e_1, e_2, ..., e_n$ di $V$ se $A$ è la matrice associata alla forma $\beta_q$. Allora sia $x = \sum_{i=1}^{n} x_i e_i$, avremo che*

$$q(x) = x^t Ax = \sum_{i,j=1}^{n} x_i x_j a_{ij}$$

*Se cambiamo base $e'_1, ..., e'_n$ di $V$ con $e'_i = Pe_i$ otteniamo la matrice $A' = P^t AP$ e in particolare si ha*

$$det(A') = det(P^t AP) = det(P)^2 det(A)$$

Dunque $det(A)$ è determinato a meno di moltiplicazione per un quadrato in $K$. Possiamo definire un invariante per $q$ nel segeuente modo:

**Definizione 3.5.** *Il discriminante di $q$ è la classe in $K/K^{*2}$ di $det(A)$ dove $A$ è la matrice associata a $q$ in una base fissata.*

**Osservazione 3.4.** *Una forma quadratica in $n$ variabili è un polinomio omogeneo di secondo grado*

$$f(X_1, X_2, ..., X_n) = \sum_{i=1}^{n} a_{ii} X_i^2 + 2 \sum_{i<j} a_{ij} X_i X_j = X^t AX$$

*Dove $A = (a_{ij})$ è una matrice simmetrica. Per ogni polinomio $f$ come sopra, diremo che il modulo standard $(K^n, f)$ è il modulo quadratico associato ad $f$.*

**Definizione 3.6.** *Una isometria tra i moduli quadratici $(V, q)$ e $(V', q')$ è una applicazione lineare $\phi : V \longrightarrow V'$ tale che*

$$\phi(v) \cdot \phi(u) = v \cdot u$$

*Per ogni $v, u \in V$. Due moduli $(V, q)$ e $(V', q')$ si dicono isometrici se hanno la stessa dimensione ed esiste una isometria $\phi$ da $V$ in $V'$.*

Si noti che una isometria tra due moduli quadratici non degeneri è sempre iniettiva. Infatti $\phi(x) = 0$ implica che $\phi(x) \cdot \phi(y) = 0 = x \cdot y$ per ogni $y \in V$ se e solo se $x = 0$. Poichè gli spazi in questione hanno dimensione finita, dire che i moduli non degeneri $(V, q)$ e $(V, q')$ sono isometrici implica in particolare l'esistenza di un isomorfismo di spazi vettoriali $\phi$ da $V$ a $V'$.

**Definizione 3.7.** *Diremo che due forme quadratiche $f$ e $f'$ sono equivalenti e scriveremo $f \sim f'$ se i moduli quadratici ad esse associati sono isometrici.*

Sia allora $A$ la matrice associata a $(K^n, f)$ e $A'$ la matrice associata a $(K^n, f')$. Vale $f \sim f'$ se e solo se esiste una matrice invertibile su $K$, che denotiamo con $M$, tale che $(Mx)^t A'(My) = x^t Ay$ se e solo se $x^t M^t A' My = x^t Ay$ per ogni $x, y \in K^n$ se e solo se $M^t A' M = A$.

## 3.2 Ortogonalità e vettori isotropi

Sia $(V, q)$ un modulo quadratico. Indicheremo d'ora in poi la forma bilineare simmetrica indotta da $q$ come $\beta_q(x, y) = x \cdot y$.

**Definizione 3.8.** *Due vettori $x, y \in V$ si dicono ortogonali e si scrive $x \perp y$ se $x \cdot y = 0$. Sia $S \subseteq V$ un sottoinsieme, l'ortogonale di $S$ è l'insieme $S^\perp$ di tutti i vettori $v$ ortogonali ad $s$, $\forall\ s \in S$.*

**Osservazione 3.5.** *Dato un sottoinsieme $S$ di $V$, il suo ortogonale $S^\perp$ è un sottospazio e vale $S^\perp = \langle S \rangle^\perp$.*

*Dimostrazione.* Siano $x_1, x_2 \in S^\perp$, $s \in S$, allora $(\lambda_1 x_1 + \lambda_2 x_2) \cdot s = \lambda_1(x_1 \cdot s) + \lambda_2(x_2 \cdot s) = 0$ e ciò mostra che l'ortogonale di $S$ è un sottospazio. Si noti ora che, se $S \subseteq T$, allora $T^\perp \subseteq S^\perp$. Perciò vale l'inclusione $\langle S \rangle^\perp \subseteq S^\perp$. Viceversa sia $x \in S^\perp$ e siano $s_1, s_2 \in S, \lambda_1, \lambda_2 \in K$, allora $x \cdot (\lambda_1 s_1 + \lambda_2 s_2) = \lambda_1(x \cdot s_1) + \lambda_2(x \cdot s_2) = 0$. □

**Definizione 3.9.** *Chiameremo radicale di $V$ il suo ortogonale e scriveremo $rad(V) = V^\perp$. La sua codimensione è detta rango di $(V, q)$. Vale allora che $(V, q)$ è non degenere se e solo se $rad(V) = \langle 0 \rangle$.*

**Definizione 3.10.**

1. *Siano $U, W \subseteq V$ due sottospazi, diremo che $U$ e $W$ sono ortogonali se $U \subseteq W^\perp$ (ed anche $W \subseteq U^\perp$).*

2. *Siano $U_1, U_2, ..., U_m \subseteq V$ sottospazi vettoriali. Diremo che $V$ è la somma ortogonale degli $U_i$ e scriveremo*
$$V = U_1 \widehat{\oplus} U_2 \widehat{\oplus} ... \widehat{\oplus} U_m$$
*se gli $U_i$ sono a due a due ortogonali e $V$ è la somma diretta $V = \bigoplus_{i=1}^m U_i$.*

3. *Viceversa siano $(U_1, q_1), (U_2, q_2), ..., (U_m, q_m)$ dei moduli quadratici, allora la somma diretta $V = \bigoplus_{i=1}^m U_i$ è canonicamente dotata di una forma quadratica $q$ definita ponendo $q(x_1, ..., x_m) = q_1(x_1) + q_2(x_2) + ... + q_m(x_m)$ per ogni $x_i \in U_i$. Gli $U_i$ sono chiaramente ortogonali e $V = U_1 \widehat{\oplus} U_2 \widehat{\oplus} ... \widehat{\oplus} U_m$.*

**Definizione 3.11.** *Siano $f(X_1, X_2, ..., X_n)$ e $g(X_1, X_2, ..., X_m)$ due forme quadratiche, indichiamo con $f + g$ la forma quadratica in $n + m$ variabili*

$$f(X_1, X_2, ..., X_n) + g(X_{n+1}, ..., X_{n+m})$$

*associata alla somma ortogonale dei moduli quadratici $(K^n, f)$ e $(K^m, g)$. Analogamemte si definisce la $f - g$ come la forma quadratica $f + (-g)$.*

**Proposizione 3.4.** *Sia $(V, q)$ un modulo quadratico non degenere, $U \subseteq V$ un sottospazio. Allora $U^{\perp\perp} = U$ e $dim(U) + dim(U^\perp) = dim(V)$.*

*Dimostrazione.* Mostro che $dim(U) + dim(U^\perp) = dim(V)$. Fissata una base $e_1, e_2, ..., e_k$ di $U$, la completo ad una base $e_1, e_2, ..., e_n$ di $V$. Sia $x = \sum_{i=1}^n x_i e_i$. Il vettore $x \in U^\perp$ se e solo se $x \cdot e_i = 0\ \forall i$, se e solo se, detta $A$ la matrice associata a $q$, $x^t A e_i = 0$, per $i = 1, .., k$. Otteniamo quindi un sistema di $k$ equazioni linearmente indipendenti che ha

come soluzione un sottospazio vettoriale di dimensione $n-k$, cioè $dim(U^\perp) = n-k = dim(V) - dim(U)$.
Infine risulta evidente che $U \subseteq (U^\perp)^\perp$ e vale l'uguaglianza perché le due hanno la stessa dimensione per quanto mostrato sopra. □

**Proposizione 3.5.** *Sia $U \subseteq V$ un sottospazio. Sono equivalenti:*

1. *$(U, q)$ è non degenere*
2. *$U \cap U^\perp = \langle 0 \rangle$*
3. *$U \widehat{\oplus} U^\perp = V$*

*Dimostrazione.* Mostro che 1. $\Rightarrow$ 2. Sia $(U, q)$ non degenere e sia $u \in U \cap U^\perp$. Allora $u \cdot x = 0$ per ogni $x \in U$ e ciò implica che $u = 0$. 2. $\Rightarrow$ 3. segue dalla Prosizione 3.4 : la formula sulle dimensioni ci dice che $U + U^\perp = V$, e se la loro intersezione è vuota la somma è diretta e quindi ortogonale. Infine siano $U \widehat{\oplus} U^\perp = V$. Se esistesse $u \in U$ tale che $u \cdot x = 0$ per ogni $x \in U$, avremmo $u \in U \cap U^\perp$ e ciò contraddice il fatto che la somma è diretta. L'implicazione 3. $\Rightarrow$ 1. è dimostrata e si conclude. □

**Definizione 3.12.** *Sia $(V, q)$ un modulo quadratico non degenere e $x \in V$. Diremo che $x$ è isotropo se $q(x) = x \cdot x = 0$. Un sottospazio $U \subseteq V$ è isotropo se lo sono tutti i suoi elementi.*

**Definizione 3.13.** *Sia $f(X_1, ..., X_n)$ una forma quadratica e $a \in K^*$. Diremo che $f$ rappresenta $a$ se esiste $x \in K^n$ tale che $f(x) = a$.*
*Diremo che $f$ rappresenta lo zero se esiste $x \in K^n$, $x \neq 0$, tale che $f(x) = 0$. In particolare $f$ rappresenta zero se il modulo quadratico ad essa associata ammette un vettore isotropo non nullo.*

**Definizione 3.14.** *Sia $V$ uno spazio vettoriale di dimensione 2 su $K$, $q$ una forma quadratica su $V$ non degenere. Se esiste un vettore $u_0 \in U$ isotropo diremo che $(V, q)$ è un piano iperbolico.*

Ogni piano iperbolico $(V, q)$ è isomorfo al piano iperbolico standard $(K^2, Q)$ dove $Q$ è definita come $Q(X_1, X_2) = X_1 X_2$ ed ha matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Infatti basta trovare una opportuna base $f_1, f_2$ di $V$. Scelgo $u_0$ isotropo e poiché $q$ è non degenere esiste $y \in V$ tale che $u_0 \cdot y = 1$. I due sono linearmente indipendenti (altrimenti si avrebbe $u_0 \cdot y = u_0 \cdot \lambda u_0 = 0$) e possiamo porre $f_1 = u_0$ ed $f_2 = 2y - q(y)u_0$. Ma allora possiamo dare la seguente definizione:

**Definizione 3.15.** *Una forma quadratica $f(X_1, X_2)$ si dice iperbolica se*

$$f \sim Q(X_1, X_2) = X_1 X_2$$

**Proposizione 3.6.** *Sia $(V, q)$ modulo quadratico e $u_0 \in V$ isotropo. Allora esiste un sottospazio $U \subseteq V$ che è un piano iperbolico.*

*Dimostrazione.* Come sopra scelgo $y \in V$ tale che $u_0 \cdot y = 1$ e $u_1 = 2y - q(y)u_0$. Allora $U = \langle u_0, u_1 \rangle$ è il sottospazio cercato. □

**Corollario 3.1.** *Sia $(V, q)$ un modulo quadratico non degenere. Se esiste un vettore isotropo $q(V) = K$, cioè per ogni $a \in K$ esiste $x \in V$ tale che $q(x) = a$.*

*Dimostrazione.* Per la proposizione precedente, esiste un piano iperbolico e sia $f_1, f_2$ la sua base come nel modello standard. Fissato $a \in K$, ho che $q(f_1 + \frac{a}{2} f_2) = a$. □

**Corollario 3.2.** *Sia $f$ una forma quadratica non degenere che rappresenta zero. Allora $f \sim f_1 + g$ dove $f_1$ è iperbolica. Inoltre $f$ rappresenta $a$ per ogni $a \in K$.*

*Dimostrazione.* Segue immediatamente dal Proposizione 3.6 e dal Corollario 3.1 □

## 3.3 Basi ortogonali

**Definizione 3.16.** *Sia $(V, q)$ un modulo quadratico. Una base $e_1, e_2, ..., e_n$ di $V$ è detta ortogonale se i suoi elementi sono a due a due ortogonali, cioè $e_i \cdot e_j = 0 \ \forall i \neq j$.*

La matrice $A$ associata a $q$ rispetto a questa base è diagonale:

$$A = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & a_n \end{pmatrix}$$

Se $x = \sum_{i=1}^{n} x_i e_i$, allora $q(x) = \sum_{i=1}^{n} a_i x_i^2$.

**Teorema 3.1.** *Ogni modulo quadratico $(V, q)$ ammette una base ortogonale.*

*Dimostrazione.* Se $q$ è la forma nulla è banale. Sia ora $q \neq 0$. Mostriamo il teorema per induzione su $n$, dove $n$ è la dimensione di $V$. Se $n = 1$ l'enunciato è ovvio. Sia $n > 1$. Esistono $v, w \in V$ tali che $w \cdot v \neq 0$. Allora almeno uno tra $v$,$w$ e $v + w$ è non isotropo. Infatti se $q(w) = q(v) = 0$, si ha $q(v + w) = (v + w) \cdot (v + w) = q(v) + q(w) + 2(v \cdot w) = 2v \cdot w \neq 0$. Pongo allora $e_1$ uguale ad uno tra $v, w$ e $v + w$ non isotropo. Allora la restrizione di $q$ a $\langle e_1 \rangle$ è non degenere e per la Proposizione 3.5 si ha che $\langle e_1 \rangle \widehat{\oplus} \langle e_1 \rangle^{\perp} = V$. Inoltre $dim \langle e_1 \rangle^{\perp} = n - 1$. Per ipotesi induttiva $(\langle e_1 \rangle^{\perp}, q)$ ammette una base ortogonale $e_2, e_3, ..., e_n$, che si completa alla base $e_1, e_2, ..., e_n$ di $V$ che costituisce dunque una base ortogonale. □

Il Teorema 3.1 si traduce nel seguente enunciato:

**Proposizione 3.7.** *Ogni forma quadratica $f(X_1, X_2, ..., X_n)$ è equivalente ad una somma di quadrati, ovvero esistono $a_1, a_2, ..., a_n$ tali che $f \sim a_1 X_1^2 + a_2 X_2^2 + .... + a_n X_n^2$.*

Si noti che allora il discriminante di $q$ è $d(q) = a_1 a_2 ... a_n$ e il rango di $q$ è dato dal numero di $a_i$ non nulli.

## 3.4 Il teorema di cancellazione

**Teorema 3.2** (Witt)**.** *Siano $(V, q)$ e $(V', q')$ due moduli quadratici non degeneri ed isometrici. Sia $U \subseteq V$ un sottospazio e $s : U \longrightarrow V'$ una isometria iniettiva. Allora $s$ si estende ad una isometria $s' : V \longrightarrow V'$.*

*Dimostrazione.* La dimostrazione si sviluppa in tre passi.

1. Si noti che l'ipotesi che $s$ sia iniettiva non è superflua, perché può accadere che $(U, q)$ sia degenere. Mostriamo allora che nel caso in cui $(U, q)$ è degenere, $s$ si estende ad una isometria $s_1$ definita su un sottospazio $U_1$ di $V$ contenente $U$ tale che la restrizione di $q$ ad $U_1$ sia non degenere. Sia $(U, q)$ degenere, cioè $U \cap U^\perp \neq \langle 0 \rangle$, e scelgo $u_0 \in U$ tale che $u_0 \cdot v = 0$ per ogni $v \in U$. Sia $W$ sottospazio tale che $U = \langle u_0 \rangle \oplus W$. Da $W \subset U$, trovo un $y \in W^\perp \setminus U^\perp$ tale che $y \cdot u_0 \neq 0$. Non è restrittivo supporre che valga $y \cdot u_0 = 1$ e (a meno di considerare $y - \frac{q(y)}{2} u_0$) $y \cdot y = 0$. Analogamente considero un sottospazio $W' \subseteq V'$ tale che $s(U) = s(u_0) \oplus W'$. Scelgo un $y' \in W'^\perp$ tale che $y' \cdot s(u_0) \neq 0$ e come prima non è restrittivo supporre $s(u_0) \cdot y' = 1$ e $y' \cdot y' = 0$. Considero $U_0 = U \oplus \langle y \rangle$ e $s_0 : U_0 \longrightarrow V'$ definita ponendo $s_0(u + \lambda y) = s(u) + \lambda y'$. Allora $s_0$ è isometria. Infatti siano $u + \lambda y$ e $v + \mu y$ in $U_0$ con $u, v \notin \langle u_0 \rangle$, allora

$$(u + \lambda y) \cdot (v + \mu y) = u \cdot v + \lambda y \cdot v + \mu y \cdot u + (\lambda\mu) y \cdot y = u \cdot v$$

e

$$\begin{aligned} s_0(u + \lambda y) \cdot s_0(v + \mu y) &= (s(u) + \lambda y') \cdot (s(v) + \mu y') \\ &= s(u) \cdot s(v) + \lambda y' \cdot s(v) + \mu y' \cdot s(u) + (\lambda\mu) y' \cdot y' \\ &= s(v) \cdot s(u) = u \cdot v \end{aligned}$$

Invece se $u = \alpha u_0$:

$$(\alpha u_0 + \lambda y) \cdot (v + \mu y) = \alpha u_0 \cdot v + \lambda y \cdot v + (\alpha\mu) y \cdot u_0 + (\lambda\mu) y \cdot y = (\alpha\mu) u_0 \cdot y = \alpha\mu$$

e

$$\begin{aligned} s_0(\alpha u_0 + \lambda y) \cdot s_0(v + \mu y) &= (s(\alpha u_0) + \lambda y') \cdot (s(v) + \mu y') \\ &= \alpha s(u_0) \cdot s(v) + \lambda y' \cdot s(v) + (\alpha\mu) y' \cdot s(u_0) + (\lambda\mu) y' \cdot y' \\ &= \alpha u_0 \cdot v + (\alpha\mu) y' \cdot s(u_0) = \alpha\mu \end{aligned}$$

E così via negli altri casi, il che mostra che $s_0(v) \cdot s_0(w) = v \cdot w$ per ogni $v, w \in U_0$. Il sottospazio $U_0$ così costruito contiene $U$ e $u_0 \notin U_0 \cap U_0^\perp$. Applico lo stesso argomento ad $u_1 \in U_0 \cap U_0^\perp$ e ad $s_0$ e procedo iterativamente fino a d esaurire i vettori indipendenti in $U \cap U^\perp$, in tal modo si determina un sottospazio $U_1$ di $V$ che contiene $U$ e una isometria $s_1$ che estende $s$ tale che $(U_1, q)$ sia non degenere.

2. Per quanto mostrato al punto 1, possiamo ora ridurci al caso in cui $(U, q)$ è non degenere e $s : U \longrightarrow V$ isometria. Vale la seguente proprietà:

**Lemma 3.1.** *Sia $(V, q)$ un modulo quadratico e $v, w \in V$ tali che $v \cdot v \neq 0 \neq w \cdot w$. Allora esiste una isometria $\sigma : V \longrightarrow V$ tale che $\sigma(v) = w$*

Siano infatti $v$ e $w$ come nel lemma. Allora almeno uno tra $x = v + w$ e $y = v - w$ è non isotropo. Infatti se $x$ è isotropo ho $x \cdot x = v \cdot v + w \cdot w + 2v \cdot w = 0$ e $y \cdot y = v \cdot v + w \cdot w - 2v \cdot w = 2v \cdot v + 2w \cdot w \neq 0$, cioè $y$ è non isotropo. Considero allora la decomposizione $V = \langle y \rangle \widehat{\oplus} \langle y \rangle^{\perp}$. Un elemento $z \in V$ si scrive come $z = u + \lambda y$ con $\lambda = \frac{y \cdot z}{y \cdot y}$ e $u = z - \frac{y \cdot z}{y \cdot y} y \in \langle y \rangle^{\perp}$. Sia $\sigma_y : V \longrightarrow V$ la simmetria rispetto a $\langle y \rangle^{\perp}$, i.e. $\sigma_y : u + \lambda y \longrightarrow u - \lambda y$, cioè $\sigma_y(z) = z - 2\frac{y \cdot z}{y \cdot y} y$. Allora $\sigma_y$ è isometria e $\sigma_y(2v) = \sigma_y(x + y) = x - y = 2w$ quindi $\sigma_y(v) = w$. Ponendo quindi $\sigma = \sigma_y$ si conclude. Se invece $y$ è isotropo, considero, come sopra, la decomposizione $V = \langle x \rangle \widehat{\oplus} \langle x \rangle^{\perp}$ e la simmetria $\sigma_x : V \longrightarrow V$ rispetto a $\langle x \rangle^{\perp}$. Allora $\sigma_x(2v) = \sigma_x(x + y) = -x + y = -2w$, quindi se pongo $\sigma = -\sigma_x$ ho conlcuso.

3. Possiamo ora mostrare il Teorema di Witt, supponendo che $(U, q)$ sia non degenere, per induzione sulla dimensione di $U$. Se $dim U = 1$, allora $U = \langle x \rangle$ e $x$ è non isotropo cioè vale $x \cdot x \neq 0$. Per ipotesi $V$ e $V'$ sono isometrici, dunque sia $f : V \longrightarrow V'$ isometria. Allora $f(x) \cdot f(x) = x \cdot x \neq 0$ e $s(x) \cdot s(x) = x \cdot x \neq 0$. Quindi $f(x)$ e $s(x)$ verificano le ipotesi del Lemma 3.1: esiste una isometria $\sigma$ definita su tutto $V'$ tale che $\sigma(f(x)) = s(x)$. Ma allora la composta $\sigma \circ f$ è una isometria ed estende banalmente $s$. Sia ora $dim U = n > 1$ e sia $x_1, x_2, ..., x_n$ una base ortogonale di $U$. Allora $U = \langle x_1, x_2, ..., x_{n-1} \rangle \widehat{\oplus} \langle x_n \rangle = U_1 \widehat{\oplus} \langle x_n \rangle$. Allo stesso modo, poiché $s$ è isometria si ha che $s(U) = U' = \langle s(U_1) \rangle \widehat{\oplus} \langle s(x_n) \rangle = \langle U_1' \rangle \widehat{\oplus} \langle s(x_n) \rangle$. Per ipotesi induttiva la restrizione di $s$ a $U_1$, $s : U_1 \longrightarrow U_1'$, si estende ad una isometria $\sigma_1 : V \longrightarrow V'$. Se $\sigma_1(x_n) = s(x_n)$ ho concluso. Siano invece $\sigma_1(x_n) \neq s(x_n)$. Si noti che, poiché $s$ e $\sigma_1$ sono isometrie, i vettori $s(x_n)$ e $\sigma_1(x_n)$ appartengono all'ortogonale di $s(U_1) = \sigma_1(U_1) = U_1'$, dunque anche i vettori $x = s(x_n) + \sigma_1(x_n)$ e $y = s(x_n) - \sigma_1(x_n)$. Inoltre sono verificate le ipotesi del Lemma 1.3. Esiste allora $\sigma_2 : V' \longrightarrow V'$ tale che $\sigma_2(\sigma_1(x_n)) = s(x_n)$ e tale $\sigma_2$ induce per costruzione l'identità su $U_1'$. Ma allora l'isometria $\sigma_2 \circ \sigma_1$ ha le proprietà richieste.

□

**Corollario 3.3.** *Sia $(V, q)$ un modulo quadratico non degenere, $U_1$ e $U_2$ sottospazi isometrici di $V$, allora i loro complementi ortogonali sono tra loro isometrici.*

*Dimostrazione.* Sia $s : U_1 \longrightarrow U_2$ isometria. Per il teorema precedente $s$ si estende ad una isometria $s' : V \longrightarrow V$ che è dunque automorfismo. Vale che $s'(U_1^{\perp}) = U_2^{\perp}$. Infatti sia $x \in U_1^{\perp}$ e $u_2 \in U_2$, allora $u_2 = s(u_1) = s'(u_1)$ per qualche $u_1 \in U_1$, dunque $s'(x) \cdot u_2 = s'(x) \cdot s(u_1) = x \cdot u_1 = 0$, cioè $s'(U_1^{\perp}) \subseteq U_2^{\perp}$. Viceversa sia $y \in U_2^{\perp}$, allora $y = s'(x)$ per qualche $x \in V$. Ne consegue che $x \cdot u_1 = s'(x) \cdot s'(u_1) = y \cdot s'(u_1) = 0$ per ogni $u_1 \in U_1$, poiché $s'(u_1) = s(u_1) \in U_2$, ovvero $U_2^{\perp} \subseteq s'(U_1^{\perp})$. Allora posso considerare la restrizione agli ortogonali $s' : U_1^{\perp} \longrightarrow U_2^{\perp}$ che è l'isometria cercata. □

Il Teorema di Witt si traduce nel seguente corollario:

**Corollario 3.4** (Teorema di cancellazione)**.** *Siano $f = f_1 + f_2$ e $g = g_1 + g_2$ due forme quadratiche, tali che $f \sim g$ e $f_1 \sim g_1$. Allora anche $f_2 \sim g_2$.*

Enunciamo ora due importanti risultati.

**Proposizione 3.8.** *Sia $g = g(X_1, X_2, ..., X_n)$ una forma quadratica non degenere su un campo $K$ e sia $a \in K^*$. Le seguenti affermazioni sono equivalenti:*

1. *$g$ rappresenta $a$*
2. *$g \sim h + aZ^2$ dove $h$ è una forma in $n-1$ variabili*
3. *$f = g - aZ^2$ rappresenta 0*

*Dimostrazione.* L'implicazione 2. $\Rightarrow$ 1. è presto verificata: il vettore $(0, 0, ..., 0, 1) \in K^n$ verifica $h(0, 0, .., 0) + a = a$, dunque la forma $h + aZ^2$ rappresenta $a$, allora $g$ che è ad essa equivalente rappresenta $a$. Per l'implicazione inversa 1. $\Rightarrow$ 2., osserviamo che esiste un $x \in V = K^n$ tale che $g(x) = a$, cioè $x \cdot x = a$. Sia $W$ il complemento ortogonale di $x$, allora $V = W \widehat{\oplus} \langle x \rangle$. Sia $h$ la restrizione di $g$ a $W$, allora $g \sim h + aZ^2$. La 2. $\Rightarrow$ 3. è evidente ed, infine, se $f = g - aZ^2$ rappresenta 0, esiste $(x_1, .., x_n, z)$ non banale tale che $g(x_1, .., x_n) + az^2 = 0$. Se $z = 0$ allora $g$ rappresenta 0 e per il Corollario 3.2 rappresenta ogni altro elemento di $K^*$, dunque anche $a$. Se $z \neq 0$ allora $g(\frac{x_1}{z}, \frac{x_2}{z}, ..., \frac{x_n}{z}) = a$ e ciò conclude la dimostrazione di 3. $\Rightarrow$ 1. □

**Proposizione 3.9.** *Siano $g$ ed $h$ due forme quadratiche non degeneri e sia $f = g - h$. Le seguenti affermazioni sono equivalenti:*

1. *$f$ rappresenta 0*
2. *esiste $a \in K^*$ che è rappresentato sia da $g$ che da $h$*
3. *esiste $a \in K^*$ tale che $g - aZ^2$ e $h - aZ^2$ rappresentano 0*

*Dimostrazione.* La doppia implicazione 2. $\Leftrightarrow$ 3. deriva dalla proposizione precedente e la 2. $\Rightarrow$ 1. è triviale. Viceversa, uno zero di $f = g - h$ può essere scritto nella forma $(x, y)$ e verfica $g(x) = h(y) = a$. Se $a \neq 0$ la tesi è verificata. Se $a = 0$, $g$ ed $h$ rappresentano 0 e quindi tutti gli altri elementi di $K^*$ per il Corollario 3.2. □

# Capitolo 4

# Il teorema di Hasse-Minkowski

## 4.1 Forme quadratiche su $\mathbb{Q}_p$

In questa sezione indicheremo con $K$ il campo dei numeri $p$-adici $\mathbb{Q}_p$ per $p$ primo. Sia $(V, q)$ un modulo quadratico su $K$. Abbiamo già introdotto il *rango* e il *discriminante* della una forma quadratica $q$, che sono invarianti perché derivano rispettivamente dal rango e dalla classe in $K^*/K^{*2}$ del determinante della matrice associata $A$ a $q$, i quali non dipendono dalla base scelta. In particolare fissata una base ortogonale di $V$, $e = (e_1, e_2, ..., e_n)$, posto $a_i = e_i \cdot e_i$ per $i = 1, 2..., n$ si ha che

$$q \sim a_1X_1^2 + a_2X_2^2 + ... + a_nX_n^2$$

e il discriminante di $q$ è

$$d(q) = a_1a_2a_3...a_n \in K^*/K^{*2}$$

Diamo ora la seguente definizione:

**Definizione 4.1.** *Si definisce il simbolo di $q$, $\varepsilon_e(q)$, come*

$$\varepsilon_e(q) = \prod_{i<j}(a_i, a_j)$$

*dove $(a_i, a_j)$ è il simbolo di Hilbert di $a_i$ e $a_j$ su $K$, definito nel Capitolo 2.*

**Proposizione 4.1.** *Sia $(V, q)$ un modulo quadratico, il simbolo di $q$ è un invariante, cioè $\varepsilon_e(q) = \varepsilon(q)$ non dipende dalla base ortogonale $e = (e_1, e_2, ..., e_n)$ scelta.*

Per poter procedere alla dimostrazione della Proposizione 4.1 è opportuno dare la definizione di basi contigue.

**Definizione 4.2.** *Sia $(V, q)$ un modulo quadratico e siano $e = (e_1, e_2, ...e_n)$ ed $e' = (e'_1, e'_2, ...e'_n)$ due basi ortogonali. Diremo che $e$ ed $e'$ sono contigue se esistono $i$ e $j$ tali che $e_i = e'_j$.*

Vale il seguente lemma:

**Lemma 4.1.** *Sia $(V, q)$ un modulo quadratico non degenere di dimensione maggiore o uguale a 3 su un campo $K$ di $char(K) \neq 2$ e siano $e = (e_1, e_2, ...e_n)$ ed $e' = (e'_1, e'_2, ...e'_n)$ due basi ortogonali. Allora esiste una sequenza $e^{(0)}, e^{(1)}, ..., e^{(r)}$ di basi ortogonali tali che $e^{(0)} = e$, $e^{(r)} = e'$ e $e^{(i)}$ è contigua con $e^{(i+1)}$.*

*Dimostrazione.* Distinguiamo tre casi:

1. $(e_1 \cdot e_1)(e'_1 \cdot e'_1) - (e_1 \cdot e'_1)^2 \neq 0$, cioè $e_1$ e $e'_1$ generano un piano non degenere. Sia allora $P = \langle e_1, e'_1 \rangle$. Esistono dei vettori $\varepsilon_2$ e $\varepsilon'_2$ tali che $P = \langle e_1 \rangle \widehat{\oplus} \langle \varepsilon_2 \rangle$ e $P = \langle e'_1 \rangle \widehat{\oplus} \langle \varepsilon'_2 \rangle$. Poichè $P$ è non degenere considero il complemento ortogonale di $P$ e scelgo una sua base ortogonale $e''_3, e''_4, ..., e''_n$. Allora una sequenza cercata è $e^{(0)} = e$, $e^{(1)} = (e_1, \varepsilon_2, e''_3, ..., e''_n)$, $e^{(2)} = (e'_1, \varepsilon'_2, e''_3, ..., e''_n)$ ed infine $e^{(3)} = e'$.

2. $(e_1 \cdot e_1)(e'_2 \cdot e'_2) - (e_1 \cdot e'_2)^2 \neq 0$, cioè $e_1$ ed $e'_2$ generano un piano non degenere $P$. Come sopra scelgo dei vettori $\varepsilon_2$ e $\varepsilon'_1$ tali che $P = \langle e_1 \rangle \widehat{\oplus} \langle \varepsilon_2 \rangle$ e $P = \langle \varepsilon'_1 \rangle \widehat{\oplus} \langle e'_2 \rangle$ ed una base $e''_3, e''_4, ..., e''_n$ ortogonale del complemento ortogonale di P. La sequenza cercata è $e^{(0)} = e$, $e^{(1)} = (e_1, \varepsilon_2, e''_3, ..., e''_n)$, $e^{(2)} = (\varepsilon'_1, e'_2, e''_3, ..., e''_n)$ ed infine $e^{(3)} = e'$.

3. $(e_1 \cdot e_1)(e'_i \cdot e'_i) - (e_1 \cdot e'_i)^2 = 0$ per $i = 1, 2$. Allora è possibile trovare un vettore $e_\lambda = e'_1 + \lambda e'_2$ non isotropo che genera un piano non degenere con $e_1$. Infatti, $e_\lambda$ è non isotropo se e solo se $e_\lambda \cdot e_\lambda = e'_1 \cdot e'_1 + \lambda^2 e'_2 \cdot e'_2 \neq 0$. Da qui ricavo la condizione $\lambda^2 \neq -\frac{e'_1 \cdot e'_1}{e'_2 \cdot e'_2}$. Inoltre $e_\lambda$ genera un piano non degenere con $e_1$ se e solo se $(e_1 \cdot e_1)(e_\lambda \cdot e_\lambda) - (e_1 \cdot e_\lambda)^2 \neq 0$. Sviluppando:

   $$(e_1 \cdot e_1)((e'_1 + \lambda e'_2) \cdot (e'_1 + \lambda e'_2)) - (e_1 \cdot (e'_1 + \lambda e'_2))^2 = -2\lambda(e_1 \cdot e'_1 + e_1 \cdot e'_2) \neq 0$$

   Otteniamo dunque $\lambda \neq 0$ e $\lambda^2 \neq -\frac{e'_1 \cdot e'_1}{e'_2 \cdot e'_2}$. Le condizioni trovate permettono di escludere tre elementi del campo $K$ e se $K$ ha più di tre elementi tale $\lambda$ può essere determinato. Se invece $K = \mathbb{F}_3$ la condizione 3. diventa $(e_1 \cdot e_1)(e'_i \cdot e'_i) = 1$ per $i = 1, 2$ perché l'unico quadrato non nullo nel campo con tre elementi è 1. Quindi otteniamo $\lambda \neq 0$ e $\lambda^2 \neq -\frac{e'_1 \cdot e'_1}{e'_2 \cdot e'_2} = -\frac{(e_1 \cdot e_1)(e'_1 \cdot e'_1)}{(e_1 \cdot e_1)(e'_2 \cdot e'_2)} = -1$ e si noti che $\lambda = 1$ verifica le condizioni richieste.
   Possiamo ora considerare $e_\lambda \in \langle e'_1, e'_2 \rangle$ e scegliere un vettore $e''_2$ tale che $\langle e_\lambda \rangle \widehat{\oplus} \langle e''_2 \rangle = \langle e'_1, e'_2 \rangle$. Allora $e'' = (e_\lambda, e''_2, e'_3, ..., e'_n)$ è una base ortogonale contigua con $e'$. Inoltre per i punti 1. e 2. posso trovare una catena di basi contigue tra $e$ ed $e''$, il che permette di concludere.

□

Possiamo ora procedere alla dimostrazione della Proposizione 4.1.

*Dimostrazione.* Ragioniamo per induzione sulla dimensione di $V$. Se $dim V = 1$ il simbolo è prodotto su un insieme vuoto di indici quindi la tesi è banalmente verificata. Se $dim(V) = 2$, siano $e_1, e_2$ una base ortogonale di $V$ e $a_i = q(e_i)$ per $i = 1, 2$. Allora per definizione $\varepsilon_e(q) = (a_1, a_2) = 1$ se e solo se la forma quadratica $Z^2 - a_1 X^2 - a_2 Y^2$ rappresenta zero, se e solo se per la Proposizione 3.8. $a_1 X^2 + a_2 Y^2$ rappresenta 1, ma ciò non dipende alla base $e$ scelta. Sia infine $n \geq 3$. In forza del Lemma 4.1 basta mostrare

la tesi per basi ortogonali $e$ ed $e'$ che sono contigue. Siano allora $e = (e_1, e_2, ..., e_n)$ ed $e' = (e'_1, e'_2, ..., e'_n)$ con $e_1 = e'_1$ e $a_i = e_i \cdot e_i$ e $a'_i = e'_i \cdot e'_i$. Per definizione

$$\begin{aligned}\varepsilon_e(q) &= (a_1, a_2)(a_1, a_3)...(a_1, a_n) \prod_{2\leq i<j} (a_i, a_j) \\ &= (a_1, a_2a_3...a_n) \prod_{2\leq i<j} (a_i, a_j) \\ &= (a_1, d(q)a_1) \prod_{2\leq i<j} (a_i, a_j)\end{aligned}$$

Allo stesso modo

$$\varepsilon_{e'}(q) = (a'_1, a'_2a'_3...a'_n) \prod_{2\leq i<j} (a'_i, a'_j) = (a'_1, d(q)a'_1) \prod_{2\leq i<j} (a'_i, a'_j) = (a_1, d(q)a_1) \prod_{2\leq i<j} (a'_i, a'_j)$$

Per ipotesi induttiva, abbiamo:

$$\prod_{2\leq i<j} (a_i, a_j) = \prod_{2\leq i<j} (a'_i, a'_j)$$

perché si tratta del simbolo della restrizione di $q$ all'ortogonale di $e_1$. Da qui si conclude che $\varepsilon_e(q) = \varepsilon_{e'}(q)$. □

Vogliamo ora studiare la rappresentabilità delle forme quadratiche su $\mathbb{Q}_p$. Ricordiamo che $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ se $p \neq 2$ e $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, dunque $K^*/K^{*2}$ ha come $\mathbb{F}_2$-spazio vettoriale un numero di elementi pari a $2^r$ dove $r = 2$ se $p \neq 2$, $r = 3$ se $p = 2$. Enunciamo il seguente lemma:

**Lemma 4.2.** *Sia $a \in K^*/K^{*2}$ e $\varepsilon = \pm 1$. Sia $H_a^\varepsilon$ l'insieme degli elementi $x \in K^*/K^{*2}$ tali che $(a, x) = 1$.*

*i. Se $a = 1$, $H_1^1$ ha $2^r$ elementi e $H_1^{-1} = \emptyset$. Se $a \neq 1$ allora $H_a^\varepsilon$ ha $2^{r-1}$ elementi.*

*ii. Siano $a, a' \in K^*/K^{*2}$ e $\varepsilon, \varepsilon' \in \{-1, 1\}$. Siano $H_a^\varepsilon$ e $H_{a'}^{\varepsilon'}$ non vuoti. Allora l'intersezione $H_a^\varepsilon \cap H_{a'}^{\varepsilon'} = \emptyset$ se e solo se $a = a'$ e $\varepsilon = -\varepsilon'$.*

*Dimostrazione.* Mostriamo la *i*. Il caso $a = 1$ è immediato, infatti, $(1, x) = 1$ per $x \in K^*/K^{*2}$ se e solo se $Z^2 - X^2 - xY^2$ ha una soluzione non triviale in $\mathbb{Q}_p^3$ e chiaramente $(1, 1, 0)$ lo è. Ma allora $H_1^1$ è tutto lo spazio e $H_1^{-1} = \emptyset$. Sia $a \neq 1$. Consideriamo l'omomorfismo

$$\begin{aligned}(a, -) : K^*/K^{*2} &\longrightarrow \{\pm 1\} \\ b &\longrightarrow (a, b)\end{aligned}$$

Allora questo ha nucleo $H_a^1$ e, ricordando che il simbolo di Hilbert è non degenere, la sua immagine è tutto $\mathbb{F}_2$, dunque è uno spazio vettoriale di dimensione 1. Quindi $H_a^1$ è un iperpiano in $K^*/K^{*2}$ ed ha $2^{r-1}$ elementi. I restanti sono $2^{r-1}$ e sono tutti e soli gli elementi di $H_a^{-1}$.
Per il punto *ii*., osserviamo che una implicazione è banale. Per l'altra, supponiamo che

$H_a^{\varepsilon} \cap H_{a'}^{\varepsilon'} = \emptyset$. Per il punto $i$. i due insiemi hanno esattamente $2^{r-1}$ elementi e sono tra loro complementari. Necessariamente si deve avere $H_{a'}^{\varepsilon'} = H_a^{-\varepsilon}$ ed allora $(a, x) = (a', x)$ per ogni $x \in K^*/K^{*2}$. Ma $(a, x) = (a', x)$ se e solo se $(a, x)(a', x) = 1$ se e solo se $(aa', x) = 1$ per ogni $x \in K^*/K^{*2}$ se e solo se, poiché il simbolo di Hilbert è non degenere, $aa' = 1$ in $K^*/K^{*2}$ cioè $a$ e $a'$ sono lo stesso elemento in $K^*/K^{*2}$. □

Sia $f$ una forma quadratica su $\mathbb{Q}_p$ di rango $n$, discriminante $d(f) = d$ e simbolo $\varepsilon(f) = \varepsilon$.

**Teorema 4.1.** *La forma quadratica $f$ rappresenta 0 se e solo se:*

*i)* $n = 2$ *e* $d = -1$

*ii)* $n = 3$ *e* $(-1, -d) = \varepsilon$

*iii)* $n = 4$ *e* $d \neq 1$ *oppure* $d = 1$ *e* $\varepsilon = (-1, -1)$

*iv)* $n \geq 5$

Prima di procedere alla dimostrazione enunciamo un immediato corollario:

**Corollario 4.1.** *Sia $a \in K^*/K^{*2}$. La forma quadratica $f$ rappresenta $a$ se e solo se:*

*i)* $n$=*1* *e* $d = a$

*ii)* $n$=*2* *e* $(a, -d) = \varepsilon$

*iii)* $n$=*3* *e* $a \neq -d$ *oppure* $a = -d$ *e* $\varepsilon = (-1, -d)$

*iv)* $n \geq 4$

*Dimostrazione.* Per la Proposizione 3.8 ragioniamo sulla forma quadratica $g = f - aZ^2$. Se il rango di $f$ è uguale ad 1, $g$ ha rango 2, dunque siamo nel caso $i$) del Teorema 4.1. La forma $g$ rappresenta 0 se e solo se $d(g) = -ad(f) = -1$ se e solo se $d(f) = d = a \in K^*/K^{*2}$. Sia ora $n = 2$, la forma quadratica $g$ ha rango 3 e, per il punto $ii$) del Teorema 4.1, rappresenta 0 se e solo se $(-1, -d(g)) = \varepsilon(g)$. Ma $d(g) = -ad(f) = -ad$ e $\varepsilon(g) = (-a, d(f))\varepsilon(f)$ quindi $(-1, ad) = (-a, d)\varepsilon$ se e solo se $(-1, ad)(-a, d) = \varepsilon$ e quindi $(-1, a)(-1, d)(-1, d)(a, d) = (a, -d) = \varepsilon$. Se $f$ ha rango 3, $g$ ha rango 4, dunque $g$ rappresenta 0 se e solo se, per la $iii$) del Teorema 4.1, $d(g) \neq 1$, e quindi $-ad \neq 1 \in K^*/K^{*2}$ ovvero $a \neq -d$, oppure $d(g) = 1$, cioè $d = -a$ e $\varepsilon(g) = (-1, -1)$ se e solo se $(-a, d)\varepsilon = (-1, -1)$ se e solo se $(d, d)(-1, -1) = \varepsilon$ se e solo se $(-1, d)(-1, -1) = \varepsilon$ ovvero $(-1, -d) = \varepsilon$. Infine, se $f$ ha rango 4, $g$ ha rango 5 e si conclude per il punto $iv$) del Teorema 4.1. □

Mostriamo ora il Teorema 4.1

*Dimostrazione.* In forza della Proposizione 3.7, scriviamo $f$ come somma di quadrati

$$f = a_1X_1^2 + a_2X_2^2 + ... + a_nX_n^2$$

dove $n$ è il rango della forma quadratica e quindi $a_i \neq 0$. Distinguiamo i casi:

1. $n = 2$ e $f = a_1X_1^2 + a_2X_2^2$. La forma $f$ rappresenta 0 se e solo se esiste $(x_1, x_2) \in K^2\backslash(0,0)$ tale che $a_1x_1^2+a_2x_2^2 = 0$ se e solo se $\frac{a_1}{a_2} = -(\frac{x_2}{x_1})^2 = -1 \in K^*/K^{*2}$. Dunque $a_1a_2$ (che appartiene alla stessa classe di $\frac{a_1}{a_2}$ in $K^*/K^{*2}$ poichè $a_1a_2 = (a_2^2)\frac{a_1}{a_2}$) appartiene alla classe di $-1$, cioè $d = a_1a_2 = -1 \in K^*/K^{*2}$.

2. $n = 3$ e $f = a_1X_1^2 + a_2X_2^2 + a_3X_3^2$. La forma quadratica $f$ rappresenta 0 se e solo se $a_3f = a_1a_3X_1^2 + a_2a_3X_2^2 + a_3^2X_3^2 \sim a_1a_3X_1^2 + a_2a_3X_2^2 + X_3^2$ rappresenta 0. Ciò accade, per definizione del simbolo di Hilbert, se e solo se $(-a_1a_3, -a_2a_3) = 1$. Ricordando che $(x, x) = (-1, x)$ e sviluppando, si ha:

$$\begin{aligned}(-a_1a_3, -a_2a_3) &= (-1,-1)(-1,a_1)(-1,a_2)(a_1,a_2)(a_1,a_3)(a_2,a_3)(-1,a_3)\\ &= (-1,-a_1a_2a_3)(a_1,a_2)(a_1,a_3)(a_2,a_3)\\ &= (-1,-d)\varepsilon = 1\end{aligned}$$

   Cioè $(-1,-d)\varepsilon = 1$ se e solo se $(-1,-d) = \varepsilon$.

3. $n = 4$ e $f = a_1X_1^2 + a_2X_2^2 + a_3X_3^2 + a_4X_4^2$. Dunque $f = a_1X_1^2 + a_2X_2^2 - (-a_3X_3^2 - a_4X_4^2)$ rappresenta 0 se e solo se, per la Proposizione 3.9, esiste un elemento $a \in K^*$ che è rappresentato dalle forme quadratiche $a_1X_1^2 + a_2X_2^2$ e $-a_3X_3^2 - a_4X_4^2$. Per il punto *ii*) del Corollario 4.1 , ciò accade se e solo se

$$(a, -a_1a_2) = (a_1, a_2) \text{ e } (a, -a_3a_4) = (-a_3, -a_4)$$

   Sia $A$ il sottoinsieme di $K^*/K^{*2}$ che verifica la prima condizione, $B$ il sottoinsieme di $K^*/K^{*2}$ che verifica la seconda condizione, allora $f$ rappresenta 0 se e solo se $A \cap B \neq \emptyset$. Per il punto *ii*. del Lemma 4.2, i due sottoinsiemi hanno intersezione vuota se e solo se $-a_1a_2 = -a_3a_4$ e $(a_1, a_2) = -(-a_3, -a_4)$. La prima condizione si traduce in $a_1a_2a_3a_4 = (a_1a_2)^2 \in K^{*2}$ cioè $d = 1$ in $K^*/K^{*2}$. Dunque $A \cap B \neq \emptyset$ se e solo se $d \neq 1$ oppure $d = 1$ e non vale la seconda condizione. Quest'ultima può essere riscritta come:

$$\begin{aligned}\varepsilon &= (a_1,a_2)(a_1,a_3)(a_1,a_4)(a_2,a_3)(a_2,a_4)(a_3,a_4)\\ &= (a_1,a_3a_4)(a_2,a_3a_4)(a_1,a_2)(a_3,a_4)\\ &= (a_1,a_2)(a_3a_4,a_3a_4)(a_3,a_4)\\ &= -(-a_3,-a_4)(-1,a_3a_4)(a_3,a_4)\\ &= -(-1,-1)(-1,a_4)(a_3,-1)(a_3,a_4)(-1,a_3)(-1,a_4)(a_3,a_4)\\ &= -(-1,-1)\end{aligned}$$

   Quindi deve valere $\varepsilon \neq -(-1,-1)$ cioè $\varepsilon = (-1,-1)$.

4. $n \geq 5$. Per il punto *ii*) del Corollario 4.1, una forma quadratica di rango 2 rappresenta gli elementi $a$ in $K^*/K^{*2}$ tali che $(a, -d) = \varepsilon$, quindi rappresenta almeno gli elementi in $H^{\varepsilon}_{-d}$, che per il Lemma 4.1 sono esattamente $2^{r-1}$. Ma allora ogni forma quadratica $f = a_1X_1^2 + ... + a_nX_n^2$ di rango $n \geq 2$ rappresenta almeno $2^{r-1}$ elementi di $K^*/K^{*2}$, e poiché $2^{r-1} \geq 2$ essa rappresenta almeno un elemento $a \in K^*/K^{*2}$ distinto da $d$. Mostriamo la tesi per $n = 5$. Per quanto appena osservato, in forza

della Proposizione 3.8, $f \sim aZ^2+g$ dove $g$ è una forma quadratica di rango 4. Allora $d(g) = \frac{d}{a} \neq 1$ in $K^*/K^{*2}$ e per il punto precedente $g$ rappresenta 0, dunque anche $f$ rappresenta 0. Il caso generale con $n > 5$ si dimostra induttivamente: $f$ rappresenta almeno un elemento $a \in K^*/K^{*2}$ quindi possiamo scrivere $f \sim aZ^2 + g$ dove $g$ è una forma quadratica di rango $n-1$ e applicando l'ipotesi induttiva si conclude.

□

Gli invarianti di rango, discriminante e simbolo introdotti permettono di classificare le forme quadratiche su $\mathbb{Q}_p$ a meno di equivalenza. Vale infatti il seguente teorema:

**Teorema 4.2.** *Siano $f$ e $g$ due forme quadratiche su $\mathbb{Q}_p$. Esse sono equivalenti se e solo se hanno lo stesso rango, discriminante $d$ e simbolo $\varepsilon$.*

*Dimostrazione.* Una implicazione è triviale: se due forme sono equivalenti esse hanno chiaramente lo stesso rango, discriminante e simbolo per definizione di questi ultimi. Il viceversa si mostra per induzione sul rango $n$ di $f$ e $g$. Se $n = 0$, si tratta della forma nulla e la tesi è banale. Sia $n \geq 1$. Per ipotesi $f$ e $g$ hanno lo stesso simbolo $\varepsilon$ e discriminante $d$. Ma allora per il Corollario 4.1 $f$ e $g$ rappresentano gli stessi elementi in $K^*/K^{*2}$. Esiste allora $a \in K^*/K^{*2}$ che è rappresentato da entrambe le forme quadratiche. Per la proposizione 3.8 si ha:

$$f \sim h + aZ^2 \text{ e } g \sim k + aZ^2$$

dove $h$ e $k$ sono forme quadratiche di rango $n-1$. Allora $d(h) = \frac{d}{a} = d(k)$ e $\varepsilon = \varepsilon(h)(a, d(h)) = \varepsilon(k)(a, d(k))$ se e solo se $d(h) = d(k)$ e $\varepsilon(h) = \varepsilon(k)$. Possiamo quindi applicare l'ipotesi induttiva: $h \sim k$ e si conclude che $f \sim h + aZ^2 \sim k + aZ^2 \sim g$. □

## 4.2 Forme quadratiche su $\mathbb{R}$

**Teorema 4.3** (Sylvester)**.** *Sia $f$ una forma quadratica reale di rango $n$. Esistono degli interi positivi $r$ ed $s$, tali che $r + s = n$ e*

$$f \sim X_1^2 + X_2^2 + ... + X_r^2 - Y_1^2 - Y_2^2 - ... - Y_s^2$$

*La coppia $(r, s)$ è detta segnatura di $f$ ed è invariante.*

*Dimostrazione.* In forza del Teorema 3.1, il modulo quadratico $(\mathbb{R}^n, f)$ ammette una base ortogonale $e_1, e_2, ..., e_n$ ed in tale base $f$ si scrive come

$$a_1X_1^2 + a_2X_2^2 + ... + a_nX_n^2$$

con $a_i \neq 0$. A meno di permutare i vettori della base, non è restrittivo supporre che esista un $r \geq 0$ tale che $a_1, a_2, ..., a_r > 0$ e $a_{r+1}, ..., a_n < 0$. Sia $e' = (e'_1, ..., e'_n)$ la base definita ponendo $e'_i = \frac{e_i}{\sqrt{|a_i|}}$. Allora

$$f \sim X_1^2 + X_2^2 + ... + X_r^2 - X_{r+1}^2 - ... - X_n^2$$

e la coppia cercata è $(r, n-r)$. Per mostrare che la segnatura non dipende dalla base scelta, considero due basi ortogonali $e = (e_1, ..., e_n)$ ed $e' = (e'_1, ..., e'_n)$, tali che $e_i \cdot e_i = 1$

per $i = 1, 2, ..., r$ e $e_i \cdot e_i = -1$ per $i = r+1, ..., n$ e $e'_j \cdot e'_j = 1$ per $j = 1, 2, .., r'$ e $e'_j \cdot e'_j = -1$ per $j = r' + 1, ..., n$. Per assurdo sia $r \neq r'$ e supponiamo $r < r'$. Allora i sottospazi $\langle e_1, e_2, ..., e_r \rangle$ e $\langle e'_{r'+1}, e'_{r'+2}, ..., e'_n \rangle$ hanno intersezione non banale, cioè esiste un $x \in \mathbb{R}^n$ tale che $x = \lambda_1 e_1 + \lambda_2 e_2 + ... + \lambda_r e_r = \mu_{r'+1} e'_{r'+1} + \mu_{r'+2} e'_{r'+2} + ... + \mu_n e'_n$. Ma allora $f(x) = \lambda_1^2 + \lambda_2^2 + ... + \lambda_r^2 = -\mu_{r'+1}^2 - \mu_{r'+2}^2 - ... - \mu_n^2$ e la prima quantità è strettamente positiva, la seconda negativa e questa è una contraddizione. □

**Osservazione 4.1.** *Diremo che la forma quadratica $f$ è definita se $r = 0$ o $s = 0$ cioè $f$ non cambia di segno, diremo che $f$ è indefinita altrimenti. In particolare $f$ è indefinita se e solo se rappresenta* 0.

## 4.3 Forme quadratiche su $\mathbb{Q}$

Come nel Capitolo 2 poniamo $V = \{p \in \mathbb{Z} \mid p \text{ è primo}\} \cup \{\infty\}$. Sia

$$f \sim a_1 X_1^2 + a_2 X_2^2 + ... + a_n X_n^2$$

una forma quadratica a coefficienti razionali di rango $n$. L'immersione di $\mathbb{Q}$ in $\mathbb{Q}_v$ permette di vedere $f$ come una forma quadratica sul campo $\mathbb{Q}_v$, $\forall v \in V$. Ad essa sono associati gli invarianti di discriminante $d_v(f) = a_1 a_2 ... a_n \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ e simbolo $\epsilon_v(f) = \prod_{i<j} (a_i, a_j)_v$, che assieme alla segnatura $(r, s)$ costituiscono gli invarianti locali della forma $f$.

**Teorema 4.4** (Hasse-Minkowski)**.** *La forma quadratica $f \in \mathbb{Q}[X_1, X_2, ..., X_n]$ rappresenta lo zero su $\mathbb{Q}$ se e solo se $f \in \mathbb{Q}_v[X_1, X_2, ..., X_n]$ rappresenta lo zero in $\mathbb{Q}_v$ per ogni $v \in V$.*

*Dimostrazione.* La necessità è ovvia: l'esistenza di uno zero globale su $\mathbb{Q}$ implica l'esistenza di zeri locali, perché $\mathbb{Q}$ si immerge in ogni completamento $\mathbb{Q}_v$. Per la sufficienza, scriviamo $f$ nella forma:

$$f = a_1 X_1^2 + a_2 X_2^2 + ... + a_n X_n^2 \quad a_i \in \mathbb{Q} \setminus \{0\}$$

A meno di considerare la forma $a_1 f$ non è restrittivo supporre che $a_1 = 1$. Trattiamo separatamente i casi $n = 2, n = 3, n = 4$ e $n \geq 5$.

1. Sia $n = 2$ e $f = X_1^2 - a X_2^2$. Si noti che poiché $f$ rappresenta lo 0 in $\mathbb{Q}_\infty = \mathbb{R}$ la forma è indefinita, dunque deve essere necessariamente $a > 0$. Scrivo $a$ nella forma:

$$a = \prod_{p \ primo} p^{ord_p(a)}$$

   La forma $f$ rappresenta 0 in $\mathbb{Q}_p$, cioè esistono $x_{1,p}, x_{2,p} \in \mathbb{Q}_p^*$ tali che $x_{1,p}^2 - a x_{2,p}^2 = 0$ cioè $a = x_{1,p}^2 x_{2,p}^{-2}$ è un quadrato in $\mathbb{Q}_p^*$. Per la Proposizione 1.8 $a = p^m u_p$ con $u_p \in \mathbb{Z}_p^*$ e $m = ord_p(a)$ pari. Ne consegue che $a$ è prodotto di potenze pari di primi, quindi è un quadrato in $\mathbb{Q}$, allora $f$ rappresenta lo 0 su $\mathbb{Q}$.

2. Sia $n = 3$ e $f = X_1^2 - a X_2^2 - b X_3^2$. A meno di moltiplicare $a$ e $b$ per quadrati possiamo supporre che $a$ e $b$ siano interi "square-free", cioè $ord_p(a)$ e $ord_p(b)$ sono uguali a

0 o a 1 per ogni primo $p$, e che $|a| \leq |b|$. Ragioniamo per induzione sull'intero $m = |a| + |b|$. Se $m = 2$, allora

$$f = X_1^2 \pm X_2^2 \pm X_3^2$$

Il caso con segni tutti positivi o negativi si esclude, perché per ipotesi $f$ rappresenta 0 su $\mathbb{Q}_\infty$, quindi è indefinita. Allora negli altri casi $f \sim X_1^2 - X_2^2 - X_3^2$ e chiaramente tale forma rappresenta lo zero su $\mathbb{Q}$. Sia ora $m > 2$. Allora $|b| \geq 2$ e scriviamo $b$ come prodotto dei suoi fattori primi $b = \pm p_1 p_2 ... p_k$. Sia $p = p_i$ e mostriamo che $a$ è un quadrato modulo $p$. Se $a = 0 \mod p$ è ovvio. Altrimenti $a$ appartiene a $\mathbb{Z}_p^*$. Per ipotesi $f$ rappresenta lo 0 su $\mathbb{Q}_p$, cioè esiste $(z, x, y) \in \mathbb{Q}_p^3 \setminus (0, 0, 0)$ tale che $z^2 - ax^2 - by^2 = 0$ e non è restrittivo assumere, per il Lemma 1.3, che $(z, x, y)$ sia primitiva. Allora $z^2 - ax^2 = 0 \mod p$. Deve essere $x \neq 0 \mod p$, infatti: se $x = 0 \mod p$ si avrebbe $z^2 = 0 \mod p$, cioè $z = 0 \mod p$. Allora $z^2 - ax^2 - by^2 = -by^2 = 0 \mod p^2$ se e solo se $y^2 = 0 \mod p^2$, poiché abbiamo supposto che $ord_p(b) = 1$. Ma allora $x = y = z = 0 \mod p$, il che contradddice il fatto che la soluzione è primitiva. Ma allora $a$ è un quadrato modulo $p_i$ per ogni $i$, quindi è un quadrato modulo $b$. Ne consegue che esistono degli interi $t$ e $b'$ tali che $t^2 - a = bb'$ e non è restrittivo scegliere $t$ tale che $|t| \leq |b|/2$. Ma allora $bb'$ è la norma di un elemento di $K(\sqrt{a})$ con $K = \mathbb{Q}$ e $K = \mathbb{Q}_v$. Per la Proposizione 2.2, $bb' \in NK_a$ implica che l'equazione $X_1^2 - aX_2^2 - bb'X_3^2$ ha una soluzione non banale, cioè $(a, bb') = 1$. Ma allora per le proprietà del simbolo di Hilbert $(a, b) = (a, bb'^2) = (a, b')$, cioè $f$ rappresenta lo zero su $K$ se e solo se la forma quadratica $f' = X_1^2 - aX_2^2 - b'X_3^2$ rappresenta lo zero su $K$. Si noti inoltre che

$$|b'| = \left| \frac{t^2 - a}{b} \right| \leq \frac{|b|}{4} + 1 < |b|$$

da $|b| \geq 2$. Scrivo $b' = b''u^2$ con $b''$ e $u$ interi e $f' \sim X_1^2 - aX_2^2 - b''X_3^2$. Ora $a$ e $b''$ sono interi square-free e $|b''| \leq |b'| < |b|$. Dunque $|a| + |b''| < m$ e, per quanto osservato sopra, $f'$ rappresenta lo 0 su $\mathbb{Q}_v$ per ogni $v \in V$. Applico l'ipotesi induttiva: $f'$ rappresenta lo zero su $\mathbb{Q}$ e quindi anche $f$.

3. Sia $n = 4$. Scriviamo f nella forma $f = a_1X_1^2 + a_2X_2^2 + a_3X_3^2 + a_4X_4^2$. Per ipotesi $f$ rappresenta lo zero in $\mathbb{Q}_v$ per ogni $v \in V$. In forza della Proposizione 3.9, esiste un $x_v \in \mathbb{Q}_v^*$ che è rappresentato da entrambe le forme $a_1X_1^2 + a_2X_2^2$ e $-a_3X_3^2 - a_4X_4^2$. Per il Corollario 4.1, ciò implica che

$$(x_v, -a_1a_2)_v = (a_1, a_2)_v \quad \text{e} \quad (x_v. - a_3a_4)_v = (-a_3, -a_4)_v$$

Per il Teorema di Hilbert valgono $\prod_{v \in V}(a_1, a_2) = 1$ e $\prod_{v \in V}(-a_3, -a_4) = 1$. Siamo sotto le ipotesi del Teorema 2.5: esiste allora un $x \in \mathbb{Q}^*$ tale che

$$(x, -a_1a_2)_v = (a_1, a_2)_v \quad \text{e} \quad (x, -a_3a_4)_v = (-a_3, -a_4)_v$$

Considero allora le forme $a_1X_1^2 + a_2X_2^2 - xZ^2$ e $a_3X_1^2 + a_4X_4^2 - xZ^2$. Applicando ancora il Corollario 4.1 si ottiene che queste rappresentano 0 in $\mathbb{Q}_v$ per ogni $v \in V$. Per il punto precedente, le due forme rappresentano lo zero su $\mathbb{Q}$ e si conclude che la forma $f$ rappresenta lo zero su $\mathbb{Q}$ per la Proposizione 3.9.

4. Sia $n \geq 5$ e $f$ una forma di rango $n$. Ragioniamo per imduzione su $n$. Scriviamo $f$ nella forma $f = h - g$ con

$$h = a_1X_1^2 + a_2X_2^2 \quad \text{e} \quad g = -(a_3x_3^2 + ... + a_nX_n^2)$$

Sia $S$ il sottoinsieme di $V$ costituito da $2, \infty$ e i primi $p$ tali che esiste un $i \geq 3$ con $ord_p(a_i) \neq 0$. Per la Proposizione 3.8, per ogni $v \in S$ esiste un $a_v$ che è rappresentato da $f$ e da $g$. Ricordando che i quadrati in $\mathbb{Q}_p^*$ formano un aperto e sfruttando la densità di $\mathbb{Q}$ in $\prod_{v \in S} \mathbb{Q}_v$, per il Lemma 2.4, posso trovare $x_1, x_2 \in \mathbb{Q}$, tali che $h(x_1, x_2) = a \in \mathbb{Q}$ tale che $a/a_v \in \mathbb{Q}_v^{*2}$ per ogni $v \in S$. Considero allora la forma quadratica $f_1 = aZ^2 - g$ e mostro che rappresenta zero in $\mathbb{Q}_v$ per ogni $v \in V$. Se $v \in S$, $g$ rappresenta $a_v$ e poiché $a/a_v \in \mathbb{Q}_p^{*2}$ rappresenta anche $a$. Se $p \notin S$, allora $a_3, a_4, ..., a_n$ sono diversi da 0 modulo $p$, quindi invertibili in $\mathbb{Z}_p$ e la riduzione modulo $p$ di $g$ è una forma quadratica di rango maggiore o uguale a 3. Ne consegue che anche il discriminante $a_3a_4...a_n \neq 0 \mod p$. Possiamo allora applicare il Corollario 2.2 e trovare uno zero non banale della riduzione modulo $p$ di $g$ e sollevarlo tramite il Corollario 1.1 ad uno zero di $g$ in $\mathbb{Q}_p$. Per il Corollario 3.2 la forma $g$ rappresenta $a$ in $\mathbb{Q}_p$. Ciò mostra che la forma $f_1$ di rango $n-1$ rappresenta lo zero in $\mathbb{Q}_v$ $\forall v \in V$. Applico l'ipotesi induttiva e trovo che $f_1$ rappresenta lo zero su $\mathbb{Q}$. Ma allora $g$ ed $h$ rappresentano $a$ su $\mathbb{Q}$ e si conclude per la Proposizione 3.9.

□

**Corollario 4.2.** *Sia $a \in \mathbb{Q}^*$. La forma quadratica $f \in \mathbb{Q}[X_1, X_2, ..., X_n]$ rappresenta $a$ in $\mathbb{Q}$ se e solo se $f \in \mathbb{Q}_v[X_1, X_2, ..., X_n]$ rappresenta $a$ in $\mathbb{Q}_v$ per ogni $v \in V$.*

*Dimostrazione.* Applico il Teorema 4.4 alla forma quadratica $aZ^2 - f$ e concludo per la Proposizione 3.8. □

**Corollario 4.3** (Teorema di Meyer)**.** *Una forma quadratica su $\mathbb{Q}$ di rango maggiore o uguale a 5 rappresenta lo zero se e solo se è indefinita.*

*Dimostrazione.* Segue dal Teorema 4.1 e 4.4 □

# Appendice A

# Il Teorema di Dirichlet sulle progressioni aritmetiche

In questa sezione daremo una dimostrazione del Teorema di Dirichlet sulle progressioni aritmetiche. Il teorema afferma che, dati due interi coprimi $a$ e $m$, esistono infiniti primi $p$ tali che $p = a \mod m$. In particolare dimostreremo che, se $m > 1$ è un intero e $a$ è primo con $m$, detto $P_a$ l'insieme dei numeri primi $p$ tali che $p = a \mod m$, vale

$$\sum_{p \in P_a} \frac{1}{p^s} \sim \frac{1}{\phi(m)} \log\left(\frac{1}{s-1}\right)$$

per $s \to 1$. Il membro a destra tende a $+\infty$ per $s \to 1$, dunque la serie $\sum_{p \in P_a} \frac{1}{p}$ diverge e ne consegue che l'insieme di indici $P_a$ è necessariamente infinito.

## A.1 Funzioni aritmetiche e serie di Dirichlet

**Definizione A.1.** *Una funzione aritmetica è una funzione $f : \mathbb{N} \longrightarrow \mathbb{C}$.*
*La funzione $f$ si dice moltiplicativa se $f(nm) = f(n)f(m)$ per ogni $n$ ed $m$ coprimi.*
*Infine, $f$ si dice strettamente moltiplicativa se $f(nm) = f(n)f(m)$ per ogni $n, m \in \mathbb{N}$.*

**Osservazione A.1.** *La funzione di Eulero $\phi(n)$ che associa ad $n$ il numero di interi positivi $m < n$ coprimi con $n$ è moltiplicativa.*

**Definizione A.2.** *Sia $f$ una funzione aritmetica e $s \in \mathbb{C}$. La serie di Dirichlet con coefficienti $f(n)$ è*

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

**Osservazione A.2.** *Sia $s = \sigma + it \in \mathbb{C}$. Se $\sigma > a$, $|n^s| = n^\sigma > n^a$ e allora $\left|\frac{1}{n^s}\right| < \frac{1}{n^a}$. Ne consegue che se la serie $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ converge assolutamente per $\sigma = a$ allora converge assolutamente per ogni $s \in \mathbb{C}$ con $\sigma > a$.*

**Proposizione A.1.** *Sia $f(n)$ limitata e $s = \sigma + it$. La serie di Dirichlet $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ converge assolutamente nel semipiano $\sigma > 1$.*

*Dimostrazione.* Sia $|f(n)| \leq K$, allora

$$\sum_{n=1}^{\infty}\left|\frac{f(n)}{n^s}\right| \leq \sum_{n=1}^{\infty}\frac{K}{n^\sigma} \leq K\sum_{n=1}^{\infty}\frac{1}{n^\alpha}$$

che converge per $\alpha > 1$. □

**Proposizione A.2.** *Sia $f$ una funzione aritmetica moltiplicativa tale che $\sum_{n=1}^{\infty} f(n)$ è assolutamente convergente. La somma della serie può essere espressa mediante il prodotto infinito convergente:*

$$\sum_{n=1}^{\infty} f(n) = \prod_{p\ primo}(1 + f(p) + f(p^2) + ... + f(p^n) + ...)$$

*In particolare se $f$ è strettamente moltiplicativa vale*

$$\sum_{n=1}^{\infty} f(n) = \prod_{p\ primo}\frac{1}{1 - f(p)}$$

*Dimostrazione.* Consideriamo il prodotto

$$P(x) = \prod_{p\leq x\ primo}\left(1 + f(p) + f(p^2) + ... + f(p^n) + ...\right)$$

Riarrangiando i termini troviamo che un generico termine del prodotto è della forma $f\left(p_1^{\alpha_1}\right) f\left(p_2^{\alpha_2}\right) ... f\left(p_r^{\alpha_r}\right) = f\left(p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}\right)$ poiché $f$ è moltiplicativa. Sia $A(x)$ l'insieme degli $n$ naturali aventi fattori primi minori o uguali ad $x$. Allora ciascun $f(n)$ si scriverà come sopra quindi: $P(x) = \sum_{n\in A(x)} f(n)$. Allora

$$\sum_{n=1}^{\infty} f(n) - P(x) = \sum_{n\in B} f(n)$$

Dove $B$ è l'insieme degli $n$ aventi un fattore primo maggiore di $x$. Si ha

$$\left|\sum_{n=1}^{\infty} f(n) - P(x)\right| \leq \sum_{n\in B}|f(n)| \leq \sum_{n\geq x}|f(n)| \to 0 \quad \text{per } x \to +\infty$$

Dalla convergenza assoluta della serie degli $f(n)$. Da qui $P(x) \to \sum_n f(n)$. Infine se $f$ è strettamente moltiplicativa vale $f(p^n) = f(p)^n$ per ogni $p$ primo, dunque si conclude ricordando che la somma di una geometrica di ragione $q$ è $\frac{1}{1-q}$. □

**Corollario A.1** (Prodotti di Eulero)**.** *Sia $f(n)$ limitata e moltiplicativa. La serie di Dirichlet $\sum_{n=1}^{\infty}\frac{f(n)}{n^s}$ converge assolutamente per $\sigma > 1$ e*

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s} = \prod_{p\ primo}\left(1 + f(p)p^{-s} + f(p^2)p^{-2s} + ... + f(p^n)p^{-ns} + ...\right)$$

*per $s = \sigma + it$ con $\sigma > 1$. Se $f$ è strettamente moltiplicativa vale*

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s} = \prod_{p\ primo}\frac{1}{1 - f(p)p^{-s}}$$

**Definizione A.3.** *Si definisce la funzione zeta come la serie di Dirichlet di $f = 1$:*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ primo}} \frac{1}{1 - p^{-s}} \quad \text{per } s = \sigma + it \in \mathbb{C} \text{ tale che } \sigma > 1$$

Enunciamo la seguente proposizione:

**Proposizione A.3.** *La funzione $\zeta(s)$ è analitica e mai nulla nel semipiano $\sigma > 1$ e ha un polo semplice in $s = 1$. Nello specifico*

$$\zeta(s) = \frac{1}{s-1} + \psi(s) \quad \text{dove } \psi \text{ è olomorfa per } \sigma > 0$$

*Dimostrazione.* Che la funzione $\zeta(s)$ sia analitica e mai nulla per $\sigma > 1$ è chiaro. Ora ricordiamo che

$$\frac{1}{s-1} = \int_1^{+\infty} t^{-s} dt = \sum_{n=1}^{\infty} \int_n^{n+1} t^{-s} dt$$

Scriviamo $\zeta(s)$ come

$$\zeta(s) = \frac{1}{s-1} + \sum_{n=1}^{\infty} \left( \frac{1}{n^s} - \int_n^{n+1} t^{-s} dt \right) = \frac{1}{s-1} + \sum_{n=1}^{\infty} \int_n^{n+1} n^{-s} - t^{-s} dt$$

Pongo $\psi_n(s) = \int_n^{n+1} n^{-s} - t^{-s} dt$ e $\psi(s) = \sum_{n=1}^{\infty} \psi_n(s)$. Resta da mostrare che $\psi$ è analitica nel semipiano $\sigma > 0$. Mostro allora che la serie $\sum_{n=1}^{\infty} \psi_n(s)$ è assolutamente convergente su ogni compatto di $\sigma > 0$.

$$|\psi_n(s)| \leq \int_n^{n+1} \left| n^{-s} - t^{-s} \right| dt \leq \sup_{n \leq t \leq n+1} \left| n^{-s} - t^{-s} \right| \leq \frac{|s|}{n^{\sigma+1}}$$

Dove ho usato il fatto che la derivata di $t^{-s}$ è $\frac{-s}{t^{s+1}}$ che ha massimo modulo uguale a $\frac{s}{n^{\sigma+1}}$ nell'intervallo $[n, n+1]$. Ma allora

$$\sum_{n=1}^{\infty} |\psi_n(s)| \leq \sum_{n=1}^{\infty} \frac{|s|}{n^{\sigma+1}} \quad \text{che converge per } \sigma > 0$$

□

**Teorema A.1.** *Per $s \to 1$ vale che:*

$$\sum_{p \text{ primo}} \frac{1}{p^s} \sim \log\left( \frac{1}{s-1} \right)$$

*Inoltre la somma $\sum_p \sum_{n \geq 2} \frac{1}{np^{sn}}$ resta limitata.*

*Dimostrazione.* Applico la funzione log a $\zeta(s)$ per $s > 1$ :

$$\begin{aligned} \log(\zeta(s)) &= \sum_{p \text{ primo}} \log\left( \frac{1}{1 - p^{-s}} \right) = \sum_{p \text{ primo}} \left( -\sum_{k=1}^{\infty} (-1)^{k+1} \frac{1}{k(-p^s)^k} \right) \\ &= \sum_{p \text{ primo}} \sum_{k=1}^{\infty} \frac{1}{kp^{ks}} = \sum_{p \text{ primo}} \frac{1}{p^s} + \Psi(s) \quad \text{dove } \Psi(s) = \sum_{p \text{ primo}} \sum_{k \geq 2} \frac{1}{kp^{sk}} \end{aligned}$$

D'altro lato $\Psi(s)$ è maggiorata da:

$$\sum \frac{1}{p^{ks}} \leq \sum \frac{1}{p^{2s}} \leq \sum \frac{1}{p^s(p^s-1))} \leq \sum \frac{1}{p(p-1)} \leq \sum_{n=1}^{\infty} \frac{1}{n(n-1)} = 1$$

Dunque è limitata anche per $s \to 1$. Allora per la Proposizione $A.3$

$$\log(\zeta(s)) = \sum_p \frac{1}{p^s} + \Psi(s) = \log\left(\frac{1}{s-1} + \psi(s)\right)$$

E mandando $s$ a 1, poichè le quantità $\Psi(s)$ e $\psi(s)$ sono limitate, si conclude che $\sum_p \frac{1}{p^s} \sim \log\left(\frac{1}{s-1}\right)$.

□

## A.2 Caratteri su gruppi abeliani finiti e caratteri modulari

Sia $G$ un gruppo abeliano finito.

**Definizione A.4.** *Un carattere su $G$ è un omomorfismo di gruppi $\chi : G \longrightarrow \mathbb{C}^*$. In particolare valgono $\chi(1_G) = 1$ e $\chi(gh) = \chi(g)\chi(h)$.*
*I caratteri su $G$ formano un gruppo, $\hat{G} = Hom(G, \mathbb{C}^*)$ detto duale di $G$.*

**Proposizione A.4.** *Sia $H \leq G$ un sottogruppo. Ogni carattere su $H$ si estende ad un carattere su $G$.*

*Dimostrazione.* Sia $H \leq G$, mostriamo l'enunciato per induzione sull'indice $(G : H)$. Se $(G : H) = 1$ allora $G = H$ e l'asserto è banale. Sia $(G : H) > 1$ e sia $x \in G$ tale che $x \notin H$. Sia $m$ il minimo intero tale che $x^m \in H$ e $\chi$ un carattere su $H$. Sia $w = \chi(x^m)$ e poiché $\mathbb{C}$ è algebricamente chiuso posso trovare un $y \in \mathbb{C}^*$ tale che $y^m = w$. Allora chiamo $H'$ il sottogruppo di $G$ generato da $H$ e da $x$. Un elemento in $H'$ si scrive come $h' = hx^\alpha$. Definisco su $H'$ la funzione $\chi'$ ponendo

$$\chi'(h') = \chi'(hx^\alpha) = \chi(h)y^\alpha$$

$\chi'$ è ben definita, è un carattere su $H'$ e chiaramente estende $\chi$. Ora $(G : H') < (G : H)$, applico l'ipotesi induttiva e concludo. □

**Proposizione A.5.** *Il gruppo $\hat{G}$ è un gruppo abeliano con lo stesso ordine di $G$.*

*Dimostrazione.* Mostriamo che $\hat{G}$ ha lo stesso ordine $n$ di $G$ per induzione su $n$. Se $n = 1$, $G$ è il gruppo banale e l'asserto è triviale. Sia $n > 1$, allora esiste $x \in G$, $x \neq 1_G$. Sia $H$ il sottogruppo ciclico generato da x, $H = \langle x \rangle$. La Proposizione 1.3 ci dice che esiste un omomorfismo $\hat{G} \longrightarrow \hat{H}$ suriettivo che induce la decomposizione $\hat{G} \simeq \hat{H} \times \hat{K}$, dove $K = G/H$. In particolare l'ordine di $\hat{G}$ è dato dal prodotto degli ordini di $\hat{H}$ e $\hat{K}$. D'altro lato se $H = \langle x \rangle$ è un gruppo ciclico di ordine $m$ e $\chi$ è un carattere su $H$, allora esso è univocamente determinato dall'immagine del generatore $\chi(x) = w \in \mathbb{C}^*$. In particolare

da $x^m = 1_H$, abbiamo che $\chi(x^m) = w^m = 1$, cioè $w$ è radice $m$-esima dell'unità. Allo stesso modo ad ogni radice $m$-esima di 1 possiamo associare un carattere $\chi \in \hat{H}$. Ma allora $\hat{H}$ ha ordine $m$, che coincide con l'ordine di $H$. D'altro lato $G/H$ ha ordine strettamente minore dell'ordine di $G$ e possiamo applicare l'ipotesi induttiva: avremo allora che l'ordine di $\hat{G}$ è uguale al prodotto degli ordini di $\hat{H}$ e $\hat{K}$, che coincide con il prodotto degli ordini di $H$ e $K = G/H$ e si conclude. □

**Proposizione A.6.** *Il gruppo $G$ è isomorfo al suo biduale $\hat{\hat{G}}$.*

*Dimostrazione.* Per ogni $x \in G$, l'applicazione $\Phi_x : \hat{G} \longrightarrow \mathbb{C}^*$, $\chi \longrightarrow \chi(x)$ è un carattere sul gruppo $\hat{G}$. Dunque è naturale definire l'omomorfismo di gruppi

$$\begin{aligned} \Phi : G &\longrightarrow \hat{\hat{G}} \\ x &\longrightarrow \Phi_x : \chi \longrightarrow \chi(x) \end{aligned}$$

Per concludere basta mostrare che $\Phi$ è iniettivo, perché per la proposizione precedente $G$ e $\hat{\hat{G}}$ hanno lo stesso ordine. Sia $x \neq 1_G$, allora $\Phi_x \neq 1$, cioè esiste $\chi \in \hat{G}$ tale che $\chi(x) \neq 1$. Questo è chiaro: considero $H = \langle x \rangle$ e, poiché $x \neq 1_G$, ha ordine $n$ maggiore di 1 dunque i suoi caratteri sono in biiezione con le radici $n$-esime dell'unità. Scelgo quindi $\chi' \in \hat{H}$ tale che $\chi'(x) \neq 1$, questo si estende per la Proposizione A.4 ad un carattere $\chi$ definito su tutto $G$, i che permette di concludere. □

**Proposizione A.7.** *Sia $G$ un gruppo abeliano finito di ordine $n$ e $\chi \in \hat{G}$. Allora*

$$\sum_{x \in G} \chi(x) = \begin{cases} n & \text{se } \chi = 1 \\ 0 & \text{altrimenti} \end{cases}$$

*Dimostrazione.* Il caso $\chi = 1$ è banale. Sia $\chi \neq 1$ e scelgo $y \in G$ tale che $\chi(y) \neq 1$. Vale

$$\sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(xy) = \sum_{x \in G} \chi(x)\chi(y) = \chi(y) \sum_{x \in G} \chi(x)$$

Segue che

$$(1 - \chi(y)) \sum_{x \in G} \chi(x) = 0 \text{ che implica } \sum_{x \in G} \chi(x) = 0$$

□

**Corollario A.2.** *Sia $G$ un gruppo abeliano di ordine $n$ e $x \in G$.*

$$\sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} n & \text{se } x = 1_G \\ 0 & \text{altrimenti} \end{cases}$$

*Dimostrazione.* Applico la Proposizione A.7 a $\hat{G}$ e concludo per l'identificazione $G \simeq \hat{\hat{G}}$ della Proposizione A.6. □

Sia ora $m > 0$ un intero e $(\mathbb{Z}/m\mathbb{Z})^*$ il gruppo moltiplicativo dell'anello $\mathbb{Z}/m\mathbb{Z}$. Allora $(\mathbb{Z}/m\mathbb{Z})^*$ è un gruppo abeliano di ordine $\phi(m)$, dove $\phi$ è la funzione di Eulero dell'Osservazione A.1.

**Definizione A.5.** *Un elemento $\chi$ del duale di $(\mathbb{Z}/m\mathbb{Z})^*$ è detto un carattere modulo $m$. Il carattere $\chi$ può essere esteso ad una funzione aritmetica $f : \mathbb{N} \longrightarrow \mathbb{C}$ ponendo*

$$f(n) = \begin{cases} \chi(\bar{n}) & \text{se } n \text{ è coprimo con } m \\ 0 & \text{altrimenti} \end{cases}$$

*Dove $\bar{n}$ è la riduzione modulo $m$ di $n$.*

## A.3 Funzioni $L$

**Definizione A.6.** *Sia $m \geq 1$ un intero e $\chi$ un carattere modulo $m$. La funzione $L$ associata ad esso è la serie di Dirichlet:*

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

Si noti che nella somma di cui sopra gli unici interi che danno contributo non nullo sono quelli coprimi con $m$.

**Proposizione A.8.** *Per $\chi = 1$ si ha*

$$L(s, 1) = F(s)\zeta(s) \quad \text{dove} \quad F(s) = \prod_{p/m} 1 - p^{-s}$$

*In particolare è analitica per $\sigma > 0$ e ha un polo semplice per $s = 1$.*

*Dimostrazione.* L'asserto è un'evidente conseguenza della Definizione A.3 e dell'osservazione di sopra. □

La proposizione che segue è cruciale per la dimostrazione del Teorema di Dirichlet: mostra infatti che $L(1, \chi)$ è finito per ogni $\chi \neq 1$. Obbiettivo sarà poi dimostrare che $L(1, \chi)$ è diversa da zero per $\chi \neq 1$.

**Proposizione A.9.** *Sia $\chi \neq 1$. Le serie $L(s, \chi)$ convergono per $\sigma > 0$ e convergono assolutamente per $\sigma > 1$. In particolare*

$$L(s, \chi) = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}} \qquad \text{per } s = \sigma + it \text{ tale che } \sigma > 1$$

*Dimostrazione.* Il caso della convergenza assoluta nel semipiano $\sigma > 1$ deriva dalla Proposizione A.2 e Corollario A.1. Per mostrare l'enunciato con $\sigma > 0$ ci serviamo dei seguenti lemmi:

**Lemma A.1** (Lemma di Abel)**.** *Siano $(a_n)_{n\in\mathbb{N}}$ e $(b_n)_{n\in\mathbb{N}}$ due successioni. Posto $A_n = \sum_{k=1}^{n} a_n$, vale:*

$$\sum_{k=m}^{n} a_k b_k = A_n b_n - A_{m-1} b_m + \sum_{k=m}^{n-1} A_k (b_k - b_{k+1})$$

*Dimostrazione.* Vale:

$$\begin{aligned}\sum_{k=m}^{n} a_k b_k &= \sum_{k=m}^{n}(A_k - A_{k-1})b_k = A_n b_n - A_{m-1}b_m + \sum_{k=m}^{n-1} A_k b_k - \sum_{k=m+1}^{n} A_{k-1}b_k \\ &= A_n b_n - A_{m-1}b_m + \sum_{k=m}^{n-1} A_k b_k - \sum_{j=m}^{n-1} A_j b_{j+1} \\ &= A_n b_n - A_{m-1}b_m + \sum_{k=m}^{n-1} A_k(b_k - b_{k+1})\end{aligned}$$

□

**Lemma A.2.** *Sia $(a_n)_{n\in\mathbb{N}}$ una successione tale che le somme parziali $S_{m,n} = \sum_{k=m}^{n} a_k$ sono limitate. Allora la serie $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converge nel semipiano $\sigma > 0$.*

*Dimostrazione.* Sia $K > 0$ tale che $|S_{m,n}| \leq K$. Mostriamo che la serie di cui sopra è di Cauchy e concludiamo per la completezza di $\mathbb{C}$. Applico il Lemma A.1 con $A_n = S_{0,n}$ e $b_n = n^{-s}$.

$$\begin{aligned}\left|\sum_{k=m}^{n} \frac{a_k}{k^s}\right| &= \left|\frac{S_{0,n}}{n^s} - \frac{S_{0,m-1}}{m^s} + \sum_{k=m}^{n-1} S_{0,k}\left(\frac{1}{k^s} - \frac{1}{(k+1)^s}\right)\right| \\ &\leq \left|\frac{S_{0,n}}{n^s}\right| + \left|\frac{S_{0,m-1}}{m^s}\right| + \left|\sum_{k=m}^{n} |S_{0,k}|\left(\frac{1}{k^s} - \frac{1}{(k+1)^s}\right)\right| \\ &\leq K\left(\left|\frac{1}{n^s}\right| + \left|\frac{1}{m^s}\right| + \left|\sum_{k=m}^{n-1} \frac{1}{k^s} - \frac{1}{(k+1)^s}\right|\right) \\ &= 2K\left(\left|\frac{1}{m^s}\right| + \left|\frac{1}{n^s}\right|\right) = \frac{2K}{m^\sigma} + \frac{2K}{n^\sigma} \to 0 \quad \text{per } m \to \infty\end{aligned}$$

Se supponiamo che $\sigma > 0$. □

In forza del Lemma A.2 basta mostrare che le somme parziali $S_{n,n'} = \sum_{k=n}^{n'} \chi(k)$ sono limitate. Se $n' - n = m$ allora per la Proposizione A.7

$$\sum_{k=n}^{n+m-1} \chi(k) = 0 \quad \text{quindi} \quad S_{n,n+m-1} = 0$$

Quindi basta maggiorare $|S_{n,n'}|$ per $n' - n < m$ e chiaramente vale

$$|S_{n,n'}| \leq \sum_{k=n}^{n'} |\chi(k)| \leq \phi(m)$$

□

**Proposizione A.10.** *Vale $L(1,\chi) \neq 0$ per ogni $\chi \neq 1$.*

Per procedere alla dimostrazione della Proposizione A.10 è opportuno introdurre la seguente funzione:

**Definizione A.7.** *Sia $m \geq 1$ un intero. Definiamo*

$$\zeta_m(s) = \prod_{\chi} L(s, \chi) \quad \textit{dove } \chi \textit{ varia tra i caratteri modulo } m$$

Sia ora $p$ un primo che non divide $m$ e sia $\bar{p}$ la sua immagine in $\mathbb{Z}/m\mathbb{Z}$. Poniamo $f(p)$ l'ordine di $\bar{p}$ in $(\mathbb{Z}/m\mathbb{Z})^*$ e $g(p) = \phi(m)/f(p)$. In particolare $g(p)$ coincide con l'ordine del gruppo quoziente $(\mathbb{Z}/m\mathbb{Z})^*/\langle\, \bar{p}\, \rangle$. Vale il seguente lemma:

**Lemma A.3.** *Se $p$ non divide $m$, si ha:*

$$\prod_{\chi}(1 - \chi(p)T) = \left(1 - T^{f(p)}\right)^{g(p)} \tag{A.1}$$

*dove $\chi$ varia tra i caratteri modulo $m$.*

*Dimostrazione.* Sia $W$ l'insieme delle radici $f(p)$-esime dell'unità. Vale

$$\prod_{w \in W}(1 - wT) = \left(1 - T^{f(p)}\right)$$

Considero il sottogruppo $H = \langle\, \bar{p}\, \rangle$ di $(\mathbb{Z}/m\mathbb{Z})^*$. I caratteri su $H$ sono in biiezione con le radici $f(p)$-esime dell'unità e per la Proposizione A.4 si estendono a caratteri modulo $m$. Allora per ogni $w \in W$ esiste un carattere $\chi$ tale che $\chi(p) = w$, in particolare i caratteri con questa proprietà sono in numero $\phi(m)/f(p) = g(p)$. Da queste osservazioni la formula A.1 segue facilmente. □

**Lemma A.4.** *La funzione $\zeta_m(s)$ è analitica per $\sigma > 1$ e*

$$\zeta_m(s) = \prod_{p \nmid m} \frac{1}{\left(1 - \frac{1}{p^{sf(p)}}\right)^{g(p)}} \tag{A.2}$$

*Dimostrazione.* La funzione $\zeta_m(s)$ è il prodotto finito delle serie di Dirichlet $L(s, \chi)$ al variare di $\chi$ tra i caratteri modulo $m$: per le Proposizioni A.8 e A.9 le $L(s, \chi)$ covergono nel semipiano $\sigma > 1$ dunque lo stesso vale per $\zeta_m$. La formula A.2 si dimostra applicando il lemma precedente con $T = \frac{1}{p^s}$:

$$\zeta_m(s) = \prod_{\chi} L(s, \chi) = \prod_{\chi}\prod_{p} \frac{1}{1 - \chi(p)p^{-s}} = \prod_{p} \frac{1}{\left(1 - p^{-sf(p)}\right)^{g(p)}}$$

□

Possiamo ora mostrare la Proposizione A.10.

*Dimostrazione.* Supponiamo per assurdo che esista un carattere modulo $m$, $\bar{\chi}$ tale che $L(1,\bar{\chi}) = 0$. Allora $\zeta_m(s) = L(s,1)L(s,\bar{\chi})\prod_{\chi\neq 1,\bar{\chi}} L(s,\chi)$ con $L(s,1)$ che ha un polo semplice per $s=1$ e $L(1,\bar{\chi})$ uno zero per $s=1$. Ma allora la funzione $\zeta_m$ ha ordine non negativo in $s=1$ ed è dunque analitica in $s=1$. Per le proposizioni A.8 e A.9 si ha che $\zeta_m(s)$ è quindi analitica per $\sigma > 0$. Tuttavia, applicando la formula A.2, si trova che il $p$-esimo fattore del prodotto è

$$\begin{aligned}\frac{1}{\left(1-\frac{1}{p^{sf(p)}}\right)^{g(p)}} &= \left(1+p^{-sf(p)}+p^{-2sf(p)}+...\right)^{g(p)} \\ &\geq \left(1+p^{-s\phi(m)}+p^{-2s\phi(m)}+...\right) \\ &= \frac{1}{1-p^{-s\phi(m)}}\end{aligned}$$

Quindi gli addendi della serie $\zeta_m(s)$ maggiorano quelli della serie

$$\sum_{(n.m)=1} \frac{1}{n^{s\phi(m)}} \sim \sum_{n=1}^{\infty} \frac{1}{n^{s\phi(m)}}$$

Che converge se e solo se $s\phi(m) > 1$. Dunque $\zeta_m(s)$ diverge per $s = \frac{1}{\phi(m)} > 0$ e questa è una contraddizione. □

## A.4 Il teorema di Dirichlet

Sia $m \geq 1$. Per ogni carattere $\chi$ modulo $m$, definiamo

$$f_\chi(s) = \sum_{p\nmid m} \frac{\chi(p)}{p^s} \quad \text{per } \sigma > 1$$

Enunciamo il seguente lemma preliminare:

**Lemma A.5.** *Valgono:*

1. *Se* $\chi = 1$, $f_1(s) \sim \log\left(\frac{1}{s-1}\right)$ *per* $s \to 1$.
2. *Se* $\chi \neq 1$, $f_\chi(s)$ *è limitata per* $s \to 1$.

*Dimostrazione.* La 1. è una conseguenza del Teorema A.1: se $\chi = 1$ ho $f_1(s) = \sum_{p|m} \frac{1}{p^s}$ che differisce da $\sum_p \frac{1}{p^s}$ per un numero finito di termini e quindi le due hanno lo stesso comportamento per $s \to 1$. Per mostrare la 2. suppongo $\chi \neq 1$ e applico la funzione log alla sua funzione $L$ associata, $L(s,\chi)$.

$$\begin{aligned}\log\left(L(s,\chi)\right) &= \sum_p \log\left(\frac{1}{1-\frac{\chi(p)}{p^s}}\right) = \sum_p \sum_{n=1}^{\infty} \frac{\chi(p)^n}{np^{sn}} \\ &= \sum_p \frac{\chi(p)}{p^s} + \sum_{p,n\geq 2} \frac{\chi(p)^n}{np^{sn}} \\ &= f_\chi(s) + F_\chi(s)\end{aligned}$$

Ora $F_\chi(s)$ è maggiorata dalla serie

$$\sum_p \sum_{n\geq 2} \frac{1}{np^n}$$

che per il Teorema A.2 è limitata per $s \to 1$. D'altro lato per la proposizione A.10 $L(s,\chi)$ è limitata e diversa da zero per $s$ che tende a 1, dunque $\log(L(s,\chi))$ è finito. Ne consegue che $f_\chi(s) = \log(L(s,\chi)) - F_\chi(s)$ è limitato per $s \to 1$. □

**Teorema A.2** (Dirichlet)**.** *Sia $m \geq 1$ un intero e $a$ un intero coprimo con $m$. Sia $P_a$ l'insieme dei primi $p$ tali che $p = a \mod m$. Allora*

$$\sum_{p\in P_a} \frac{1}{p^s} \sim \frac{1}{\phi(m)} \log\left(\frac{1}{s-1}\right) \quad \textit{per } s \to 1$$

*In particolare l'insieme $P_a$ è infinito.*

*Dimostrazione.* Vale

$$\sum_{p\in P_a} \frac{1}{p^s} = \frac{1}{\phi(m)} \sum_\chi \chi(a)^{-1} f_\chi(s) \tag{A.3}$$

dove $\chi$ varia tra i caratteri modulo $m$. Infatti

$$\sum_\chi \chi(a)^{-1} f_\chi(s) = \sum_\chi \chi(a)^{-1} \sum_p \frac{\chi(p)}{p^s} = \sum_p \sum_\chi \frac{\chi(a^{-1}p)}{p^s}$$

Per il Corollario A.2, $\sum_\chi \chi(a^{-1}p) = \phi(m)$ se e solo se $a^{-1}p = 0 \mod m$ cioè $p = a \mod m$, altrimenti la somma è nulla, cioè

$$\sum_\chi \chi(a)^{-1} f_\chi(s) = \phi(m) \sum_{p\in P_a} \frac{1}{p^s}$$

Mandiamo $s$ a 1 nella formula A.3 e applichiamo il Lemma A.5. Per $\chi \neq 1$, la quantità $\chi(a)^{-1} f_\chi(s)$ è limitata, dunque il comportamento della serie è dato da $f_1 \sim \log\left(\frac{1}{s-1}\right)$ e si conclude. □

# Bibliografia


[1] Tom M Apostol. *Introduction to analytic number theory*. Springer Science & Business Media, 1998.

[2] Keith Conrad. *The local-global principle*.

[3] Kazuya Kato, Nobushige Kurokawa, and Takeshi Saitō. *Number Theory: Fermat's dream*. AMS Bookstore, 2000.

[4] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, volume 58. Springer Science & Business Media, 2012.

[5] E Sernesi. *Geometria 1*. Bollati Boringheri, Torino, 1992.

[6] Jean-Pierre Serre. *A course in arithmetic*, volume 7. Springer Science & Business Media, 2012.