Università degli Studi di Pisa

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E DELLA NATURA
Corso di Laurea Triennale in Matematica

Tesi di laurea triennale

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

Candidato:
Giacomo Hermes Ferraro
Matricola 548963

Relatore:
Davide Lombardo

Anno Accademico 2017–2018

Indice

Introduzione

La ricerca di soluzioni intere di equazioni a coefficienti interi, o equazioni diofantee, è un problema matematico con una lunga storia e di non facile risoluzione. Uno degli approcci principali consiste nel considerare le equazioni di partenza modulo n per qualche numero naturale $n \geq 2$: rendendo finiti i casi da controllare, si facilita la ricerca di eventuali soluzioni. Questo metodo si rivela particolarmente utile per dimostrare l'assenza di soluzioni intere; ad esempio, si può partire dalla seguente equazione: $x^2+y^4+1 = 4z^3$. Lavorando modulo 4 si ottiene l'equazione $x^2+y^4+1 \equiv_4 0$, ed è immediato osservare che, poiché gli unici quadrati modulo 4 sono 0 e 1, l'equazione non può avere soluzione modulo 4, e dunque a maggior ragione non può avere soluzioni intere. Ben più complesso è il problema per così dire opposto: se esistono soluzioni di un'equazione diofantea modulo n per ogni numero naturale $n \geq 2$, è sempre vero che l'equazione ammette anche soluzioni intere? In generale la risposta è no (alcuni controesempi verranno presentati nel capitolo 5), ed è un problema di particolare interesse e difficoltà determinare per quali classi di equazioni diofantee la risposta è affermativa.

Grazie al teorema cinese del resto, se n ha fattorizzazione unica $p_1^{a_1} \cdots p_k^{a_k}$, un'equazione ammette soluzione modulo n se e solo se ne ammette una modulo $p_i^{a_i}$ per i che va da 1 a k, dunque è sufficiente lo studio dell'equazione modulo le potenze dei numeri primi. Questa osservazione conduce allo studio dei $\mathbb{Q}_p$, detti *campi p-adici*, e dei loro sottoanelli $\mathbb{Z}_p$, i cui elementi sono invece detti *interi p-adici*. Infatti, tra le peculiarità di queste costruzioni (che saranno presentate nel capitolo 1) c'è la proprietà che, dato un polinomio a coefficienti interi, questo ha uno zero in $\mathbb{Z}_p$ se e solo se ha uno zero modulo p^n per ogni $n \geq 1$. Se una data classe di equazioni gode della proprietà che ogni suo elemento ammette soluzione in ogni $\mathbb{Z}_p$ se e solo se ammette soluzione in $\mathbb{Z}$ (oppure che ammette soluzione in ogni $\mathbb{Q}_p$ se e solo se ammette soluzione in $\mathbb{Q}$), si dice che per quella classe di equazioni vale il *principio locale-globale*.

Un primo contesto in cui il principio locale-globale è valido sono i sistemi lineari, e in questo paragrafo se ne darà una breve illustrazione, nella forma più debole in cui l'esistenza di una soluzione modulo p^n per ogni p e per ogni $n \geq 1$ implica l'esistenza di una soluzione razionale. Un sistema lineare a coefficienti interi può essere scritto come $Ax = b$, dove A è una matrice a coefficienti interi, b è il vettore dei termini noti, e x è un vettore le cui componenti sono le incognite del sistema. Per il teorema di Rouché-Capelli, se il sistema non ammette soluzioni su $\mathbb{Q}$, deve valere $rk(A|b) > rk(A)$. In particolare, se $rk(A) = k$, tutti i minori $(k+1) \times (k+1)$ della matrice A devono avere determinante nullo, mentre esiste un minore M della matrice $(A|b)$ di dimensioni $(k+1) \times (k+1)$ il cui determinante è $d \neq 0$. Se ora considero il sistema modulo p, dove p è un primo che non divide d, varrà ancora $rk(A) \leq k$, mentre il determinante di M non sarà congruo a 0 modulo p, per cui si avrà $rk(A|b) \geq k+1$. In particolare, valendo ancora $rk(A|b) > rk(A)$, non può esistere una soluzione al sistema modulo p.

La classe successiva di equazioni per cui si può sperare che valga il principio locale-globale sono le forme quadratiche su $\mathbb{Q}$, ossia i polinomi omogenei di secondo grado in un certo numero di variabili a coefficienti in $\mathbb{Q}$. In effetti, anche in questo caso la risposta è affermativa, e questo

risultato (noto come *teorema di Hasse-Minkowski* e decisamente più complesso del caso lineare) sarà il fulcro di questa trattazione: nel capitolo 3 verrà dimostrato che una forma quadratica ammette uno zero non banale su $\mathbb{Q}$ se e solo se ne ammette uno su ogni $\mathbb{Q}_p$ e su $\mathbb{R}$, mentre nel capitolo 6 verranno presentati alcuni degli strumenti necessari a generalizzare questo risultato da $\mathbb{Q}$ ad ogni campo di numeri.

Alla luce del teorema di Hasse-Minkowski, è naturale chiedersi se il principio locale-globale sia valido anche per polinomi di grado più alto. Tuttavia il principio, sia nella formulazione presentata sopra sia in formulazioni più fini, fallisce anche in casi relativamente semplici, e questo sarà il soggetto del capitolo 5.

Infine, poiché la dimostrazione del teorema di Hasse-Minkowski fa uso della legge di reciprocità quadratica, e i controesempi richiedono il teorema di reciprocità cubica o l'uso di strumenti che compaiono nella sua dimostrazione, il capitolo 4 sarà dedicato a presentare questi due risultati.

Capitolo 1

Preliminari

Per approfondimenti sugli argomenti trattati nella prima e nella seconda sezione di questo capitolo, si rimanda rispettivamente a [Coh07, cap.4] e [Coh07, cap.5].

1.1 I campi p-adici

1.1.1 Valore assoluto e completamento di un campo

Per poter parlare di campi p-adici è necessario introdurre il concetto di *valore assoluto*.

Definizione 1.1.1. Sia $\mathbb{K}$ un campo qualsiasi. Una funzione $\|\cdot\| : \mathbb{K} \to \mathbb{R}$ è detta *valore assoluto* se rispetta le seguenti proprietà.

Definitezza **:** $\forall x \in \mathbb{K}$ si ha $\|x\| \geq 0$ e $\|x\| = 0$ se e solo se $x = 0$.

Moltiplicatività **:** $\forall x, y \in \mathbb{K}$ si ha che $\|xy\| = \|x\| \cdot \|y\|$.

Disuguaglianza triangolare generalizzata **:** $\exists c \in \mathbb{R}_{>0}$ tale che $\|x + y\|^c \leq \|x\|^c + \|y\|^c \ \forall x, y \in \mathbb{K}$.

Ai fini della trattazione, si considereranno i valori assoluti per cui $c = 1$, poiché tutti gli altri si ricavano da questi elevando ad una potenza opportuna. Inoltre, non verrà considerato il valore assoluto banale, ottenuto imponendo $\|x\| = \begin{cases} 1 \text{ se } x \in \mathbb{K}^* \\ 0 \text{ se } x = 0 \end{cases}$.

Definizione 1.1.2. Un valore assoluto $\|\cdot\|$ su un campo $\mathbb{K}$ di caratteristica 0 è detto *archimedeo* se esiste $m \in \mathbb{Z}$ tale che $\|m\| > 1$. Altrimenti, è detto *non archimedeo*.

Poiché ad ogni valore assoluto corrisponde una metrica sul campo di riferimento, è naturale la seguente definizione:

Definizione 1.1.3. Due valori assoluti $\|\cdot\|_1$ e $\|\cdot\|_2$ su un campo $\mathbb{K}$ sono detti equivalenti se sono equivalenti come norme su $\mathbb{K}$, ossia se inducono la stessa topologia; l'insieme dei valori assoluti a meno di equivalenza è detto insieme dei *posti* di $\mathbb{K}$.

Considerando su $\mathbb{K}$ la topologia indotta da un valore assoluto, vale il seguente risultato:

Proposizione 1.1.4. *La somma e il prodotto sono operazioni continue, viste come applicazioni da* $\mathbb{K} \times \mathbb{K}$ *in* $\mathbb{K}$ *(dove su* $\mathbb{K} \times \mathbb{K}$ *si considera l'usuale topologia prodotto).*

Nel caso in cui $\mathbb{K}$ sia un campo di numeri, ossia un'estensione algebrica finita di $\mathbb{Q}$, esistono due modi naturali di ricavare un valore assoluto. Il primo parte dall'osservazione che ogni elemento di un campo di numeri $\mathbb{K}$ può essere scritto come $\frac{x}{y}$, dove x e y sono elementi del suo anello degli interi $\mathcal{O}_{\mathbb{K}}$, dunque basta definire il valore assoluto su $\mathcal{O}_{\mathbb{K}}$ ed estenderlo a $\mathbb{K}$ per moltiplicatività (la buona definizione è immediata). Per ogni ideale primo $P \subseteq \mathcal{O}_{\mathbb{K}}$ si ha che $\bigcap_{n\in\mathbb{N}} P^n = \{0\}$, pertanto è possibile dare la seguente definizione:

Definizione 1.1.5. Sia P un ideale primo di $\mathcal{O}_{\mathbb{K}}$. Per ogni elemento $x \in \mathcal{O}_{\mathbb{K}}^*$ viene detta *valutazione P-adica* di x, e si scrive $v_P(x)$, l'unico numero naturale n tale che $x \in P^n \backslash P^{n+1}$ (dove $P^0 := \mathcal{O}_{\mathbb{K}}$).

Osservazione 1.1.6. Nel caso in cui $\mathbb{K} = \mathbb{Q}$ (dunque $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}$), fissato un ideale primo $P = (p) \subseteq \mathbb{Z}$ e un numero intero a, $v_P(a) = e$ se e solo se p compare con esponente e nella fattorizzazione di a. In tal caso, la valutazione P-adica è anche detta valutazione p-adica, e si può indicare con v_p.

Proposizione 1.1.7. *Sia $\mathbb{K}$ un campo di numeri e sia $P \subseteq \mathcal{O}_{\mathbb{K}}$ un ideale primo del suo anello degli interi. Allora $\forall c \in \mathbb{R}_{>1}$, $c^{-v_P(\cdot)}$ è un valore assoluto non archimedeo su $\mathbb{K}$, e i valori assoluti ottenuti in questo modo sono tutti equivalenti al variare di c.*

Si può dimostrare che, dati due ideali primi distinti P e Q, i valori assoluti da loro determinati non sono equivalenti.

Un altro modo di definire una norma moltiplicativa su un campo di numeri è mediante una norma moltiplicativa già nota, ossia la norma euclidea sui numeri complessi:

Proposizione 1.1.8. *Sia $\mathbb{K}$ un campo di numeri e $\sigma : \mathbb{K} \to \mathbb{C}$ un omomorfismo iniettivo di campi. Allora $|\sigma(\cdot)|$ è un valore assoluto archimedeo su $\mathbb{K}$ (dove $|\cdot|$ indica la consueta norma euclidea su $\mathbb{C}$).*

Si osserva che gli omomorfismi σ e $\bar{\sigma}$ danno luogo allo stesso valore assoluto. Inoltre, si può dimostrare che se σ e τ sono due omomorfismi non coniugati, i valori assoluti da loro determinati non sono equivalenti. In particolare, detta (r, s) la *segnatura* di $\mathbb{K}$ (ossia r è il numero di omomorfismi iniettivi $\mathbb{K} \to \mathbb{C}$ che hanno immagine reale e $2s$ è il numero di omomorfismi iniettivi la cui immagine non è contenuta in $\mathbb{R}$), con questo metodo è possibile trovare $r + s$ valori assoluti non equivalenti.

Un risultato importante afferma che i valori assoluti ottenuti in questi due modi sono in realtà tutti i valori assoluti definibili sul campo di numeri $\mathbb{K}$. Per la precisione si ha il seguente:

Teorema 1.1.9 (Ostrowski, [Coh07, Teorema 4.1.13])**.** *Sia $\mathbb{K}$ un campo di numeri di segnatura (r, s) e $\mathcal{O}_{\mathbb{K}}$ il suo anello degli interi. Allora, a meno di equivalenza, i suoi posti archimedei sono esattamente $r + s$, e i suoi posti non archimedei sono in corrispondenza biunivoca con gli ideali primi di $\mathcal{O}_{\mathbb{K}}$.*

Infine, per ogni posto v si può considerare il completamento del campo $\mathbb{K}$ rispetto ad una qualsiasi metrica $\|\cdot\|_v$ relativa a v: per continuità di somma e prodotto rispetto alla metrica $\|\cdot\|_v$, questo oggetto sarà ancora un campo, denotato $\mathbb{K}_v$, e $\|\cdot\|_v$ si estenderà ad un valore assoluto su questo campo. Ogni campo ottenuto mediante questa costruzione viene denominato *campo locale*.

Nel caso in cui $\mathbb{K} = \mathbb{Q}$, ogni posto v è indicato con un elemento di $P \cup \{\infty\}$, dove P è l'insieme dei numeri primi naturali. L'unico posto archimedeo è quello associato alla metrica euclidea, e il completamento relativo sarà $\mathbb{Q}_\infty = \mathbb{R}$. I completamenti non archimedei $\mathbb{Q}_p$ sono in corrispondenza con i numeri primi e vengono detti campi p-adici. Canonicamente, la norma relativa a $\mathbb{Q}_p$ è data da $\|\cdot\|_p = p^{-v_p(\cdot)}$ (per elementi diversi da 0).

Una costruzione che accompagna quella del campo p-adico $\mathbb{Q}_p$ è quella dell'anello degli *interi p-adici*.

Definizione 1.1.10. Gli *interi p-adici* $\mathbb{Z}_p$ sono la chiusura di $\mathbb{Z}$ in $\mathbb{Q}_p$ secondo la metrica p-adica.

Una facile conseguenza della definizione è che $\mathbb{Z}_p$ eredita da $\mathbb{Z}$ la struttura di anello, poiché somme e prodotti passano al limite.

Per continuità della norma, poiché secondo ogni metrica p-adica vale che, $\forall x \in \mathbb{Z}$, $\|x\|_p \leq 1$, si ha che $\mathbb{Z}_p \subseteq \{x \in \mathbb{Q}_p | \|x\|_p \leq 1\}$. In realtà vale il seguente risultato:

Proposizione 1.1.11. *Gli interi p-adici sono tutti e soli gli elementi di* $\mathbb{Q}_p$ *con norma minore o uguale a* 1.

Dimostrazione. Un'inclusione è già stata mostrata. Per l'altra, sia $x \in \mathbb{Q}_p^*$ con $\|x\|_p \leq 1$: essendo un elemento di $\mathbb{Q}_p$, esiste una successione $\{x_n\}_n \subseteq \mathbb{Q}$ che converge ad x in norma p-adica. Inoltre, per continuità della norma, $\lim_n \|x_n\|_p = \|x\|_p = 1$, ma dato che la norma può assumere solo valori in $N = \{0\} \cup \{p^n | n \in \mathbb{Z}\}$, e che 1 è un punto isolato di N, deve valere che $\|x_n\|_p = 1$ definitivamente (senza perdita di generalità assumo che questa uguaglianza valga per ogni n). Dunque x_n si può esprimere in forma di frazione come $\frac{a_n}{b_n}$, dove $a_n, b_n \in \mathbb{Z}$ e dove b_n non è multiplo di p. Questo vuol dire che b_n è invertibile modulo p^n, perciò è possibile trovare $c_n \in \mathbb{Z}$ tale che $c_n \equiv a_n b_n^{-1} \mod p^n$. Vale quindi che:

$$\left\| \frac{a_n}{b_n} - c_n \right\|_p = \left\| \frac{a_n - c_n b_n}{b_n} \right\|_p = \|a_n - c_n b_n\|_p \leq p^{-n}.$$

Da questa disuguaglianza segue che la successione $\{c_n\}_n$ e la successione $\{x_n\}_n$ convergono allo stesso valore, dunque $x = \lim_n c_n$, e pertanto appartiene alla chiusura di $\mathbb{Z}$ secondo la norma p-adica. □

Inoltre, la struttura di $\mathbb{Z}_p$ e dei suoi ideali permette di lavorare *modulo* p^n. In altri termini, valgono i seguenti risultati:

Proposizione 1.1.12. $\mathbb{Z}_p$ *è un anello locale, ossia ha un unico ideale massimale* P*, dove:*

$$P = \{x \in \mathbb{Q}_p | \|x\|_p < 1\} = \{x \in \mathbb{Q}_p | \|x\|_p \leq p^{-1}\}.$$

Inoltre, per ogni $n \in \mathbb{N}$ *si ha che* $P^n = p^n \mathbb{Z}_p$ *e vale l'isomorfismo* $\mathbb{Z}_p / P^n \cong \mathbb{Z}/p^n\mathbb{Z}$.

Una particolarità della norma sui campi p-adici è data dalla seguente proposizione, valida per generici valori assoluti:

Proposizione 1.1.13. *Sia* $\|\cdot\|$ *un valore assoluto non archimedeo su un campo* $\mathbb{K}$*. Allora vale la disuguaglianza ultrametrica:* $\|x + y\| \leq \max\{\|x\|, \|y\|\}$ *per ogni* $x, y \in \mathbb{K}$.

Questa proprietà rende la struttura topologica dei campi p-adici molto diversa da quella di $\mathbb{R}$, e ha particolari conseguenze nello studio delle serie di funzioni. Da un lato, una reinterpretazione della disuguaglianza ultrametrica è che se due palle hanno intersezione non vuota, allora sono una inclusa nell'altra: questo rende inapplicabile il concetto di prolungamento analitico di una serie di potenze, molto importante su $\mathbb{R}$ e $\mathbb{C}$. D'altronde, ci sono aspetti che vengono semplificati dalla proprietà ultrametrica.

Proposizione 1.1.14. *Sia $\{a_n\}_{n\in\mathbb{N}}$ una successione a valori in $\mathbb{Q}_p$. Allora:*

$$\sum_{n=0}^{+\infty} a_n < +\infty \iff \lim_{n\to\infty} a_n = 0;$$
$$\left\|\sum_{n=0}^{+\infty} a_n\right\|_p \leq \max_n\{\|a_n\|_p\}.$$

Corollario 1.1.15. *Sia $\sum_{n=0}^{+\infty} a_n x^n$ una serie di potenze a coefficienti in $\mathbb{Q}_p$. Il suo raggio di convergenza è:*

$$R = \frac{1}{\limsup_n \|a_n\|_p^{\frac{1}{n}}}.$$

Corollario 1.1.16. *Siano $\sum_{n=0}^{+\infty} a_n$ e $\sum_{n=0}^{+\infty} b_n$ due serie convergenti. Allora:*

$$\sum_{n=0}^{+\infty}(a_n + b_n) = \sum_{n=0}^{+\infty} a_n + \sum_{n=0}^{+\infty} b_n;$$
$$\sum_{n=0}^{+\infty}(a * b)_n = \left(\sum_{n=0}^{+\infty} a_n\right)\left(\sum_{n=0}^{+\infty} b_n\right),$$

dove $(a * b)_n$ indica l'n-esimo termine del prodotto di Cauchy tra le successioni $\{a_n\}_n$ e $\{b_n\}_n$.

Questi lemmi hanno come conseguenza che molte serie di Taylor di funzioni su $\mathbb{R}$ rimangano invariate su $\mathbb{Q}_p$. Un esempio che tornerà utile nella trattazione è il seguente:

Corollario 1.1.17. *La radice quadrata della funzione $1 + x$ ha serie di Taylor in un intorno di 0, su ogni $\mathbb{Q}_p$, espressa da:*

$$\sum_{n=0}^{+\infty} \binom{\frac{1}{2}}{n} x^n.$$

Poiché dal punto di vista formale il quadrato di questa serie coincide con la funzione $1 + x$, le proprietà precedenti implicano che la serie coincide con una radice quadrata di $1 + x$ fintanto che si ha convergenza. Per trovare il valore dei raggi di convergenza è necessario espandere i coefficienti della serie e trovarne la valutazione p-adica e si può verificare che per $p \neq 2$ la serie converge per ogni x con $v_p(x) \geq 1$, mentre per $p = 2$ converge per ogni x con $v_2(x) \geq 3$.

Per concludere la presentazione dei campi p-adici, è bene osservare qualche proprietà topologica. Come affermato nella proposizione 1.1.4, somma e prodotto sono funzioni continue da $\mathbb{Q}\times\mathbb{Q}$ in $\mathbb{Q}$ rispetto alla norma p-adica (e si estendono a funzioni continue da $\mathbb{Q}_p \times \mathbb{Q}_p$ in $\mathbb{Q}_p$): di conseguenza ogni polinomio in n variabili (e dunque anche ogni forma quadratica) è un'applicazione continua da $\bigtimes_1^n \mathbb{Q}_p$ a $\mathbb{Q}_p$.

Inoltre, la struttura metrica dei $\mathbb{Q}_p$ permette di codificare mediante la norma le congruenze modulo p^n: in questo modo, è possibile riformulare in senso topologico un risultato analogo al teorema cinese del resto:

Proposizione 1.1.18 (Lemma di approssimazione)**.** *Sia V un insieme finito di posti di $\mathbb{Q}$ e per ogni $v \in V$ sia $A_v \neq \emptyset$ un sottoinsieme aperto di $\bigtimes_1^n \mathbb{Q}$ rispetto alla topologia prodotto indotta dalla metrica $\|\cdot\|_v$. Allora l'intersezione degli A_v è non vuota.*

Dimostrazione. Dimostro prima di tutto il caso $n = 1$. Per prima cosa considero i posti diversi da ∞. Per ogni $p \in V\backslash\{\infty\}$, A_p è aperto e non vuoto, dunque in particolare esistono un elemento

$x_p \in A_p$ e un numero reale positivo r_p (che senza perdita di generalità posso prendere pari a p^{-k_p}, con k_p numero naturale) tali che la palla aperta $B_p = \{y \in \mathbb{Q} | \|y - x_p\|_p < r_p\}$ è inclusa in A_p: mi basta quindi dimostrare che l'intersezione dei B_p al variare di p è non vuota ed interseca A_∞. Per ogni $p \in V\backslash\{\infty\}$ posso scrivere $x_p = \frac{a_p}{b_p}$ come frazione ai minimi termini e definisco B il prodotto di tutti i b_p al variare di p. Fissato N intero positivo, considero tutti i numeri razionali del tipo $\frac{c}{NB}$ con c intero, e ho che:

$$\frac{c}{NB} \in B_p \Leftrightarrow \left\| \frac{c}{NB} - \frac{a_p}{b_p} \right\|_p < r_p \Leftrightarrow \left\| c - a_p \frac{NB}{b_p} \right\|_p < p^{-k_p} \|NB\|_p.$$

Noto che, essendo B multiplo di b_p, l'elemento di cui prendo la norma a sinistra dell'equazione è un numero intero. Inoltre, poiché NB è un numero intero, la sua norma p-adica sarà una certa potenza di p con esponente minore o uguale a 0. Per questo motivo, ho $p^{-k_p}\|NB\|_p = p^{-h_p}$ per un certo $h_p \geq 0$, per cui riscrivo la condizione nel modo seguente:

$$\left\| c - a_p \frac{NB}{b_p} \right\|_p < p^{-h_p} \Leftrightarrow v_p \left(c - a_p \frac{NB}{b_p} \right) > h_p \Leftrightarrow c \equiv a_p \frac{NB}{b_p} \mod p^{h_p+1}.$$

Voglio sapere quando un intero c soddisfa tutte queste congruenze al variare di $p \in V\backslash\{\infty\}$, e per il teorema cinese del resto so che ciò avviene se e solo se:

$$c \equiv a \mod M, \text{ con } M := \prod_{p \in V\backslash\{\infty\}} p^{h_p+1},$$

dove a è un opportuno numero intero. Dunque l'intersezione dei B_p contiene l'insieme:

$$I_N := \frac{a + M\mathbb{Z}}{N} = \{ \frac{a}{N} + k\frac{M}{N} | k \in \mathbb{Z}\} \subseteq \mathbb{Q}.$$

Se V non contiene ∞ ho finito; se invece lo contiene, poiché $A_\infty \neq \emptyset$ è un aperto secondo la topologia euclidea, conterrà un insieme del tipo $(x - \varepsilon, x + \varepsilon) \cap \mathbb{Q}$, con $x \in A_\infty$ e ε numero reale positivo. Posso scegliere N in modo che $\frac{M}{N}$ sia minore di 2ε: in tal modo, la distanza euclidea tra due elementi consecutivi di I_N è minore di 2ε, e pertanto uno dei suoi elementi è contenuto nell'intervallo $(x - \varepsilon, x + \varepsilon) \cap \mathbb{Q}$, e dunque in A_∞, come volevasi dimostrare.

Infine, per n generico, poiché A_v è aperto non vuoto per ogni $v \in V$, ogni A_v contiene un plurirettangolo, ossia un prodotto di aperti non vuoti di $\mathbb{Q}_v$ del tipo $A_{v,1} \times \cdots \times A_{v,n}$. Applicando il caso precedente ottengo che per ogni i l'intersezione $A_i := \bigcap_{v \in V} A_{v,i}$ è non vuota, e poiché $A_1 \times \cdots \times A_n \subseteq \bigcap_{v \in V} A_v$, anche questa intersezione è non vuota. □

1.1.2 I lemmi di Hensel

Il teorema di Hasse-Minkowski richiede di studiare l'esistenza di soluzioni per forme quadratiche sui campi p-adici e su $\mathbb{R}$. Su $\mathbb{R}$ esistono strumenti di analisi che permettono di determinare se una data funzione ammetta zeri in un certo sottoinsieme del dominio. Poiché la possibilità di utilizzare l'analisi differenziale su $\mathbb{R}$ è una conseguenza della sua completezza, è ragionevole aspettarsi di ottenere dei risultati analoghi sui campi p-adici. In effetti, lo strumento che verrà utilizzato in questa trattazione presenta diverse analogie con il metodo di Newton e con il teorema della funzione implicita.

Proposizione 1.1.19 (Lemma di Hensel-1)**.** *Sia $f \in \mathbb{Z}_p[x]$, $\overline{f}, \overline{\phi_1}, \overline{\phi_2} \in \mathbb{F}_p[x]$ tali che $f \equiv_p \overline{f}$, e $\overline{f} = \overline{\phi_1} \cdot \overline{\phi_2}$ con $\overline{\phi_1}$ e $\overline{\phi_2}$ coprimi. Allora $\exists \phi_1, \phi_2 \in \mathbb{Z}_p[x]$ tali che:*

- $\deg(\phi_1) = \deg(\overline{\phi_1})$;
- $\phi_1 \equiv_p \overline{\phi_1}$;
- $\phi_2 \equiv_p \overline{\phi_2}$;
- $f = \phi_1\phi_2$.

Dimostrazione. Dimostro per induzione che $\exists a_k, b_k, U, V \in \mathbb{Z}_p[x]$ tali che:

- $f \equiv_{p^k} a_k b_k$;
- $Ua_k + Vb_k \equiv_p 1$;
- $a_{k+1} - a_k \equiv_{p^k} b_{k+1} - b_k \equiv_{p^k} 0$;
- $\deg(a_k) = \deg(\overline{\phi_1})$;
- $\deg(b_k) \leq \deg(f) - \deg(\overline{\phi_1})$.

Per iniziare prendo a_0 e b_0 due qualsiasi rappresentanti rispettivamente di $\overline{\phi_1}$ e $\overline{\phi_2}$, con lo stesso loro grado, mentre l'esistenza di U e V è garantita dalla coprimalità dei due polinomi su $\mathbb{F}_p[x]$. Per il passo induttivo, suppongo di aver già trovato i polinomi al passo k. Scrivo quindi:

$$a_{k+1} = a_k + p^k c_k \quad \text{e} \quad b_{k+1} = b_k + p^k d_k.$$

Voglio avere:

$$f \equiv_{p^{k+1}} a_{k+1}b_{k+1} \equiv_{p^{k+1}} (a_k + p^k c_k)(b_k + p^k d_k) \equiv_{p^{k+1}} a_k b_k + p^k(a_k d_k + b_k c_k).$$

Dunque voglio trovare c_k e d_k tali che:

$$a_k d_k + b_k c_k \equiv_p \frac{1}{p^k}(f - a_k b_k) =: g_k.$$

Posso farlo per Bezout, dato che a_k e b_k sono coprimi su $\mathbb{F}_p[x]$ per induzione. In particolare, posso prendere:

$$d_k \equiv_p Ug_k + Wb_k \quad \text{e} \quad c_k \equiv_p Vg_k - Wa_k,$$

per qualche polinomio $W \in \mathbb{Z}_p[x]$. Esiste (ed è unico modulo p) un polinomio W tale che $\deg(c_k) < \deg(a_k)$, per cui scegliendo quel W ho $\deg(a_{k+1}) = \deg(a_k) = \deg(\overline{\phi_1})$. Inoltre:

$$\deg(b_k c_k) < \deg(a_k b_k) \leq \deg(f) \quad \text{e} \quad \deg(g_k) \leq \deg(f).$$

Dunque:

- $\deg(a_k d_k) \leq \deg(f)$;
- $\deg(d_k) \leq \deg(f) - \deg(\overline{\phi_1})$;
- $\deg(b_{k+1}) \leq \max\{\deg(b_k)\deg(d_k)\} \leq \deg(f) - \deg(\overline{\phi_1})$;
- $Ua_{k+1} + Vb_{k+1} \equiv_p Ua_k + Vb_k \equiv_p 1$.

A questo punto, basta prendere $\phi_1 := \lim_{k\to\infty} a_k$ e $\phi_2 := \lim_{k\to\infty} b_k$: entrambi i limiti esistono perché $\{a_k\}_k$ e $\{b_k\}_k$ sono successioni di Cauchy in norma p-adica, ed essendo limiti di polinomi a coefficienti interi, hanno i coefficienti nella chiusura di $\mathbb{Z}$, ossia in $\mathbb{Z}_p$; inoltre le condizioni modulo p e di grado sono soddisfatte per le proprietà del limite, e:

$$\phi_1\phi_2 = (\lim_{k\to\infty} a_k)(\lim_{k\to\infty} b_k) = (\lim_{k\to\infty} a_k b_k) = f.$$

□

Proposizione 1.1.20 (Lemma di Hensel-2)**.** *Sia $f \in \mathbb{Z}_p[x_1, \cdots, x_n]$. Dato un polinomio in $\mathbb{Z}_p[x_1, \cdots, x_n]$ indicherò con $\bar{\cdot}$ la sua proiezione su $\mathbb{F}_p[x_1, \cdots, x_n]$. Supponiamo che:*

$$\exists(\beta_1, \cdots, \beta_n) \in \mathbb{F}_p^n : \ \overline{f}(\beta_1, \cdots, \beta_n) = 0;$$
$$\exists i : \overline{\frac{\partial f}{\partial x_i}}(\beta_1, \cdots, \beta_n) \neq 0.$$

Allora:

$$\exists(\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}_p^n : \ f(\alpha_1, \cdots, \alpha_n) = 0, \ (\alpha_1, \cdots, \alpha_n) \equiv_p (\beta_1, \cdots, \beta_n).$$

Dimostrazione. Senza perdita di generalità $\overline{\frac{\partial f}{\partial x_1}}(\beta_1, \cdots, \beta_n) \neq 0$. Per ogni $i \neq 1$ trovo un rappresentante $\alpha_i \in \mathbb{Z}_p$ di β_i e considero il polinomio $g(x) := f(x, \alpha_2, \cdots, \alpha_n) \in \mathbb{Z}_p[x]$. Per ipotesi, ho:

$$\overline{g}(\beta_1) = 0, \ \overline{g'}(\beta_1) = \overline{\frac{\partial f}{\partial x_1}}(\beta_1, \cdots, \beta_n) \neq 0.$$

Pertanto, β_1 è una radice di molteplicità 1 di $\overline{g}$, dunque posso scrivere $\overline{g} = (x - \overline{\alpha})h(x)$, con $x - \overline{\alpha}$ e $h(x)$ coprimi. Ma allora, per il lemma di Hensel-1, esistono $p(x), q(x) \in \mathbb{Z}_p[x]$ tali che:

- $g(x) = p(x)q(x)$;
- $p(x) \equiv_p x - \overline{\alpha}$;
- $q(x) \equiv_p h(x)$;
- $\deg(p(x)) = \deg(x - \overline{\alpha}) = 1$.

In particolare, $p(x) = ax + b$ con $a, b \in \mathbb{Z}_p$ e $a \neq 0$, per cui $g\left(\frac{-b}{a}\right) = 0$ (per la precisione, poiché, quando visto modulo p, $p(x)$ ha ancora grado 1, $a \in \mathbb{Z}_p^*$, dunque $\frac{-b}{a} \in \mathbb{Z}_p$). Inoltre:

$$\frac{-b}{a} \equiv_p \frac{\overline{\alpha}}{1} \equiv_p \overline{\alpha}.$$

pertanto ho che $\left(\frac{-b}{a}, \alpha_2, \cdots \alpha_n\right) \in \mathbb{Z}_p^n$ è una soluzione di f che solleva la soluzione di $\overline{f}$: $(\beta_1, \cdots, \beta_n) \in \mathbb{F}_p^n$. □

Infine si riporta una terza versione del lemma di Hensel, più fine della precedente, che meglio evidenzia il collegamento tra l'esistenza delle soluzioni di un'equazione in un campo p-adico e l'esistenza di soluzioni modulo p^k per qualche k. Innanzitutto, è necessario dimostrare il seguente lemma.

Lemma 1.1.21 (Formula di Taylor-Lagrange per polinomi)**.** *Sia $f \in \mathbb{Z}_p[x]$ un polinomio. Allora per ogni n esiste $c \in \mathbb{Z}_p$ tale che:*

$$f(x+h) - f(x) = \left(\sum_{i=1}^{n} \frac{f^{(i)}(x)}{i!} h^i \right) + h^{n+1} c,$$

dove con $f^{(i)}$ si indica la derivata i-esima di f.

Dimostrazione. Per linearità della derivata, basta dimostrare la formula sui monomi $f(x) = x^k$. In questi casi, la dimostrazione è una banale conseguenza dell'espansione in binomio di Newton:

$$(x+h)^k = \sum_{i=0}^{k} \binom{k}{i} x^{k-i} h^i = x^k + \sum_{i=1}^{k} \frac{(x^k)^{(i)}}{i!} h^i.$$

□

Proposizione 1.1.22 (Lemma di Hensel-3)**.** *Sia $f \in \mathbb{Z}_p[x_1, \cdots, x_n]$. Supponiamo che per qualche i tra 1 e n valga la seguente:*

$$\exists \alpha \in (\mathbb{Z}/p\mathbb{Z})^n : \ \|f(\alpha)\|_p < \left\| \frac{\partial f}{\partial x_i}(\alpha) \right\|_p^2.$$

Allora esiste un'unica radice $\alpha^* \in \mathbb{Z}_p$ di $f(x_1, \cdots, x_n) = 0$ tale che $\alpha_j^* = \alpha_j$ per ogni $j \neq i$, mentre per l'i-esima coordinata vale:

$$\|\alpha_i^* - \alpha_i\|_p \leq \frac{\|f(\alpha)\|_p}{\left\| \frac{\partial f}{\partial x_i}(\alpha) \right\|_p}.$$

Dimostrazione. Per semplicità di notazione, dimostrerò solo il caso in una variabile: il caso in più variabili è del tutto analogo.

Procedo secondo il metodo della tangente di Newton e definisco ricorsivamente $\alpha_0 := \alpha$ e $\alpha_{n+1} := \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}$. Dimostro per induzione le seguenti affermazioni:

- $\|f(\alpha_{n+1})\| < \|f(\alpha_n)\|$;
- $\|f'(\alpha_{n+1})\| = \|f'(\alpha_n)\|$;
- $\|f(\alpha_{n+1})\| < \|f'(\alpha_{n+1})\|^2$.

La terza proprietà è una diretta conseguenza delle prime due e del fatto che $\|f(\alpha_0)\| < \|f'(\alpha_0)\|^2$.

Per la formula di Taylor-Lagrange per polinomi, posto $\beta_n := \alpha_{n+1} - \alpha_n = -\frac{f(\alpha_n)}{f'(\alpha_n)}$, ho che per ogni n esistono $\gamma_n, \delta_n \in \mathbb{Z}_p$ tali che:

$$\begin{aligned} f(\alpha_{n+1}) &= f(\alpha_n) + f'(\alpha_n)\beta_n + \gamma_n \beta_n^2; \\ f'(\alpha_{n+1}) &= f'(\alpha_n) + \delta_n \beta_n. \end{aligned}$$

Per la scelta di β_n, si ha $f(\alpha_{n+1}) = \gamma_n \beta_n^2$, e poiché $\|\gamma_n\| \leq 1$:

$$\|f(\alpha_{n+1})\| \leq \|\beta_n\|^2 = \frac{\|f(\alpha_n)\|^2}{\|f'(\alpha_n)\|^2} < \|f(\alpha_n)\|,$$

dove l'ultimo passaggio è conseguenza dell'ipotesi induttiva. Infine, poiché $\|\delta_n\| \leq 1$:

$$\|\delta_n \beta_n\| \leq \|\beta_n\| = \frac{\|f(\alpha_n)\|}{\|f'(\alpha_n)\|} < \|f'(\alpha_n)\|.$$

Da questo si ottiene la seconda proprietà:

$$\|f'(\alpha_{n+1})\| = \|f'(\alpha_n) + \delta_n \beta_n\| = \|f'(\alpha_n)\|.$$

Dalle proprietà appena dimostrate si deduce che la successione reale $\|\beta_n\| = \frac{\|f(\alpha_n)\|}{\|f'(\alpha_n)\|} = \frac{\|f(\alpha_n)\|}{\|f'(\alpha_0)\|}$ è strettamente decrescente, e poiché per ogni $n \in \mathbb{N}$ si ha che $\|f(\alpha_n)\| \in N := \{0\} \cup \{p^k | k \in \mathbb{N}\}$, questa successione deve tendere a 0. In particolare, anche $\lim_n \beta_n = 0$, e dunque la successione α_n è di Cauchy e ammette limite α^*. Per continuità di f rispetto alla norma p-adica si ha che $f(\alpha^*) = 0$; inoltre:

$$\|\alpha^* - \alpha\| = \left\| \sum_{n=0}^{\infty} \beta_n \right\| \leq \max_n \{\|\beta_n\|\} = \|\beta_0\| = \frac{\|f(\alpha)\|}{\|f'(\alpha)\|}.$$

□

In particolare, se si prende $k = v_p(f(\alpha))$, le ipotesi del lemma equivalgono ad avere una radice di f modulo p^k, con qualche condizione opportuna sulla valutazione p-adica della derivata.

Corollario 1.1.23. *Esistono $p-1$ radici $p-1$-esime dell'unità nel campo $\mathbb{Q}_p$, sono tutte in $\mathbb{Z}_p$, e sono tutte distinte modulo p.*

Dimostrazione. Sia n un intero compreso tra 1 e $p-1$: per il lemma di Hensel-2, poiché n è una radice del polinomio $f(x) = x^{p-1} - 1$ modulo p, e $f'(n) = (p-1)n^{p-2} \equiv_p -n^{-1} \not\equiv_p 0$, esiste una radice $\alpha_n \in \mathbb{Z}_p$ di $f(x)$ tale che $\alpha \equiv_p n$. Al variare di n tra 1 e $p-1$, si ottengono $p-1$ radici: sono tutte distinte perché diverse modulo p, e poiché $f(x)$ ha grado $p-1$, sono tutte e sole le radici $p-1$-esime dell'unità. □

Forti di questa osservazione, è possibile descrivere l'insieme dei quadrati di $\mathbb{Q}_p^*$, indicato con $\mathbb{Q}_p^{*2}$:

Proposizione 1.1.24. *$\mathbb{Q}_p^* \cong \mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^* \times U_0$, dove $U_0 := \{x \in \mathbb{Z}_p^* | v_p(x-1) \geq 1\}$. In particolare, $|\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}|$ è pari a 8 se $p = 2$ e 4 altrimenti. Inoltre, $x \in \mathbb{Q}_p^*$ è un quadrato se e solo se, posto $x = p^k x'$ con $v_p(x') = 0$, accade una delle seguenti:*

- *$p \neq 2$, $k \in 2\mathbb{Z}$ e x' è un quadrato modulo p;*
- *$p = 2$, $k \in 2\mathbb{Z}$ e $x' \equiv 1 \mod 8$.*

Dimostrazione. Mi basta mostrare che l'insieme delle potenze di p, le radici $p-1$ esime dell'unità e U_0 sono tutti sottogruppi normali con intersezione banale e che generano $\mathbb{Q}_p^*$. Che siano sottogruppi normali è ovvio per abelianità di $\mathbb{Q}_p^*$, ed è anche immediato osservare che a due a due hanno intersezione $\{1\}$, dunque basta mostrare che generano. Un qualsiasi elemento $x \in \mathbb{Q}_p^*$ si può scrivere come $x = p^n \sum_{i=0}^{\infty} a_i p^i$ dove $n \in \mathbb{Z}$ è la valutazione p-adica di x, gli a_i sono interi compresi tra 0 e $p-1$ e $a_0 \neq 0$. Per il precedente corollario esiste (ed è unica) una radice $p-1$-esima dell'unità $\alpha \in \mathbb{Z}_p$ congrua ad a_0 modulo p. Pertanto, si può scrivere, per qualche $y \in \mathbb{Z}_p$: $x = p^n \cdot \alpha \cdot (1 + py)$.

Inoltre, da quanto affermato nel corollario 1.1.3 si deduce che per $p \neq 2$ ogni elemento di U_0 è un quadrato, mentre per $p = 2$ U_0^2 consiste negli elementi di U_0 congrui a 1 modulo 8, dunque è un sottogruppo di U_0 di indice 4. La seconda parte del teorema è una banale conseguenza della struttura di $\mathbb{Q}_p^{*2}$. □

1.2 Le forme quadratiche

1.2.1 Notazioni e considerazioni utili

Definizione 1.2.1. Una *forma quadratica* su $\mathbb{K}$ è un polinomio omogeneo di secondo grado in un certo numero di variabili a coefficienti in $\mathbb{K}$.

Ogni forma quadratica in n variabili $q(x_1, \cdots, x_n)$ su un campo $\mathbb{K}$ può essere rappresentata in forma matriciale nel modo seguente: $q = x^T Ax$, dove x è il vettore n-dimensionale la cui coordinata i-esima è la variabile x_i, mentre A è una matrice $n \times n$ con coefficienti in $\mathbb{K}$. Se la caratteristica del campo è diversa da 2, poiché $x^T Ax = x^T A^T x$, è possibile sostituire la matrice A con la matrice simmetrica $Q = \frac{A+A^T}{2}$: questa sarà la matrice associata alla forma quadratica. Grazie a questo legame tra la forma quadratica q e la matrice simmetrica Q, è possibile associare a q un prodotto scalare $(\cdot, \cdot)$ sullo spazio vettoriale $\mathbb{K}^n$, dove $(x, y) := x^T Qy$. Queste considerazioni permettono le seguenti definizioni:

Definizione 1.2.2. Sia q una forma quadratica in n variabili su $\mathbb{K}$ di caratteristica diversa da 2, sia Q la matrice associata e $(\cdot, \cdot)$ il prodotto scalare corrispondente.

- Il rango della matrice Q viene detto *rango* di q.
- q è detta *non degenere* se Q ha rango massimo, ed è detta *degenere* altrimenti. In altri termini, q è degenere se e solo se esiste un vettore non nullo x tale che $\forall y \in \mathbb{K}^n$ si abbia $(x, y) = 0$.
- q è detta *isotropa* se esiste un vettore non nullo x tale che $x^T Qx = 0$, e in tal caso x è detto *vettore isotropo* di q. Se non esiste un tale x, la forma è detta *anisotropa*.
- Si dice che due forme quadratiche q e q' sono *equivalenti*, e si scrive $q \sim q'$, se esiste una matrice A invertibile tale che $q(x) = q'(Ax)$. In altri termini, dette Q e Q' le matrici associate, $q \sim q'$ se $Q = A^T Q' A$.

Dall'ultima definizione segue che se $q \sim q'$, q è isotropa se e solo se q' è isotropa: per questo motivo, dato che il teorema di Hasse-Minkowski richiede di determinare se una forma abbia o meno vettori isotropi, è utile studiare le forme quadratiche a meno di questa relazione di equivalenza. Grazie all'algoritmo di riduzione di Gauss per forme quadratiche, se il campo $\mathbb{K}$ su cui è definita la forma ha caratteristica 0, è sempre possibile trovare una matrice diagonale D e una matrice invertibile A tali che $Q = A^T DA$, dunque la forma $q'(y) := y^T Dy$ è equivalente alla forma q. Pertanto è possibile, senza perdita di generalità, studiare le sole forme quadratiche diagonali del tipo $q'(y_1, \cdots, y_n) = a_1 y_1^2 + \cdots + a_n y_n^2$: una forma di questo tipo, definita sul campo $\mathbb{K}$, verrà indicata con la notazione $\langle a_1, \cdots, a_n \rangle_{\mathbb{K}}$, mentre sarà indicata solo come $\langle a_1, \cdots, a_n \rangle$ qualora il campo base sia chiaro dal contesto. Inoltre, è immediato osservare che la forma $\langle a_1, \cdots, a_n \rangle$ è degenere se e solo se uno dei suoi coefficienti a_i è nullo.

Definizione 1.2.3. Sia q una forma quadratica su $\mathbb{K}$ e sia $c \in \mathbb{K}$. Si dice che q *rappresenta* c se esiste un vettore non nullo $x \in \mathbb{K}^n$ tale che $q(x) = c$.

I seguenti risultati sulle forme quadratiche mirano a legare la proprietà di rappresentare lo 0 con la proprietà di rappresentare un generico elemento $c \in \mathbb{K}$. Il campo base $\mathbb{K}$ verrà considerato avere caratteristica diversa da 2.

Lemma 1.2.4. *Se una forma quadratica non degenere q su $\mathbb{K}$ rappresenta lo 0, allora rappresenta ogni elemento di $\mathbb{K}$.*

Dimostrazione. Sia $(\cdot,\cdot)$ il prodotto scalare relativo alla forma q. Dato un vettore isotropo x, per la non degenerazione $\exists z \in \mathbb{K}$ tale che $(x,z) \neq 0$, quindi prendo:

$$y = \left[z - \frac{(z,z)}{(2x,z)}x\right]\frac{1}{(x,z)} \Rightarrow (y,y) = 0, (x,y) = 1.$$

Segue che $a = q\left(x + \frac{a}{2}y\right)$ per tutti gli elementi $a \in \mathbb{K}$. □

Lemma 1.2.5. *Una forma quadratica q su $\mathbb{K}$ rappresenta $c \in \mathbb{K}^*$ se e solo se $q - cx^2$ rappresenta lo 0.*

Dimostrazione. Se $q(x_1, \cdots, x_n) = c$, il vettore di coordinate $(x_1, \cdots, x_n, 1)$ è isotropo per la forma $q - cx^2$. D'altro canto se $q(x_1, \cdots, x_n) - cx^2 = 0$ e $x \neq 0$, basta dividere per x^2 e si ha $q(\frac{x_1}{x}, \cdots, \frac{x_n}{x}) = c$, mentre se $x = 0$, q rappresenta lo 0, e dunque rappresenta anche c per il lemma precedente. □

Capitolo 2

Il simbolo di Hilbert

Lo strumento principale nella dimostrazione del teorema di Hasse-Minkowski è il simbolo di Hilbert. L'idea alla base di quest'ultimo è di quantificare la considerazione qualitativa che dice se una forma quadratica ammette o meno vettori isotropi sul campo base. Si esaminerà in particolare il caso in cui tali campi base siano i completamenti di $\mathbb{Q}$ (si veda in proposito [Coh07, cap.5]). Tuttavia è bene osservare che le proprietà fondamentali sono vere per i completamenti di una qualsiasi estensione finita di $\mathbb{Q}$, ma che le dimostrazioni di alcune di esse necessitano di un approccio più astratto (cui si accennerà nel capitolo 6).

2.1 Definizione e prime proprietà

Definizione 2.1.1. Sia $ax^2 + by^2 - z^2$ una forma quadratica non degenere su un campo locale $\mathbb{Q}_v$. Il *simbolo di Hilbert* ad essa relativo si scrive $(a, b)_v$ ed è pari a 1 se la forma ha soluzione non banale in $\mathbb{Q}_v$ e a -1 altrimenti.

Per comodità, si scriverà $(\cdot, \cdot)$ senza alcun pedice nel caso in cui il campo di riferimento sia qualsiasi o sia chiaro dal contesto.

Alcune proprietà del simbolo di Hilbert seguono immediatamente dalla definizione.

Proposizione 2.1.2. *Su qualsiasi campo locale valgono le seguenti relazioni:*

- $(a, b) = (b, a)$;
- $(a, c^2) = 1$;
- $(a, -a) = 1$;
- $(a, 1 - a) = 1$;
- $(a, b) = 1$ *implica* $(a', b) = (aa', b)$, *di conseguenza:*

$$(a, b) = (a, -ab) = (a, (1 - a)b).$$

Dalla terza e dalla quinta proprietà si ricava che $(a, a) = (a, -1)$. Dalla seconda e dalla quinta proprietà segue che il simbolo di Hilbert è invariante a meno di moltiplicazione di un suo argomento per un quadrato di $\mathbb{Q}_v^*$. In particolare, è possibile considerare il simbolo di Hilbert come se fosse definito su $\mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$.

Ora l'obiettivo è di determinare una formula per il valore del simbolo di Hilbert. Prima di tutto si deve provare il seguente facile risultato:

Lemma 2.1.3. *Siano $a, b \in \mathbb{Z}_p^*$, e sia $ax^2+bpy^2-z^2 = 0$ dove $x, y, z \in \mathbb{Q}_p$ e non sono tutti nulli. Allora esistono $x', y', z' \in \mathbb{Z}_p$ non tutti nulli tali che $ax'^2 + bpy'^2 - z'^2$ e $v_p(x') = v_p(z') = 0$.*

Dimostrazione. È immediato osservare che, poiché l'equazione considerata è omogenea, si possono moltiplicare x, y e z per uno stesso fattore e ottenere tre numeri $x', y', z' \in \mathbb{Z}_p$ tali che almeno uno di loro abbia valutazione p-adica nulla e che valga ancora $ax'^2 + bpy'^2 = z'^2$. Se per assurdo $v_p(x') \geq 1$, si avrebbe che $v_p(\text{LHS}) \geq 1$, dunque anche il RHS avrebbe valutazione p-adica positiva, e quindi $v_p(z') \geq 1$ (in modo del tutto analogo si dimostra che se $v_p(z') \geq 1$ si ha anche $v_p(x') \geq 1$). Ma allora $v_p(bpy'^2) = v_p(z'^2 - ax'^2) \geq 2$, dunque $v_p(y') \geq 1$, il che è contrario all'ipotesi che uno tra x', y', z' abbia valutazione pari a 0. Pertanto deve valere $v_p(x') = v_p(z') = 0$. □

Proposizione 2.1.4 (Formula del simbolo di Hilbert)**.** *Valgono le seguenti uguaglianze per il simbolo di Hilbert $(\cdot, \cdot)_v$.*

$\boxed{v = \infty}$ $(a, b)_\infty = 1$ *se e solo se almeno uno tra a e b è positivo.*

$\boxed{p = v \neq 2, \infty}$ *Scrivo $a = a'p^\alpha$, $b = b'p^\beta$, con $a', b' \in \mathbb{Z}_p^*$. Allora:*

$$(a, b) = (-1)^{\frac{\alpha\beta(p-1)}{2}} \left(\frac{a'}{p}\right)^\beta \left(\frac{b'}{p}\right)^\alpha.$$

$\boxed{v = 2}$ *Con la stessa notazione di sopra:*

$$(a, b) = (-1)^{\frac{(a'-1)(b'-1)}{4}} (-1)^{\frac{a'^2-1}{8}\beta} (-1)^{\frac{b'^2-1}{8}\alpha}.$$

Dimostrazione. Il primo caso è banale.

Per il secondo caso, per simmetria del simbolo di Hilbert e poiché dividendo un termine del simbolo di Hilbert per un quadrato il suo valore non cambia, mi basta verificare la formula per i seguenti valori di α, β:

$\boxed{\alpha = \beta = 0}$ Voglio dimostrare che $(a', b') = 1$. È facile mostrare che l'equazione associata $a'x^2 + b'y^2 = z^2$ ha una soluzione non banale in $\mathbb{F}_p$ del tipo $(x', y', 1)$. Infatti, considero gli insiemi $\{a'x^2\}$ e $\{1 - b'y^2\}$ al variare rispettivamente di x e y in $\mathbb{F}_p$. Entrambi gli insiemi hanno cardinalità $\frac{p+1}{2}$, dunque per pigeonhole esistono x' e y' tali che $a'x'^2 = 1 - b'y'^2$. Ora, per il lemma di Hensel-2, posso sollevare a una soluzione dell'equazione in $\mathbb{Q}_p$.

$\boxed{\alpha = 0, \beta = 1}$ Voglio dimostrare che $(a', pb') = \left(\frac{a'}{p}\right)$. Per il lemma precedente, se esiste una soluzione non banale all'equazione associata in $\mathbb{Q}_p$, ce n'è una con $x, z \in \mathbb{Z}_p^*$, pertanto l'equazione $a'x^2 + pb'y^2 = z^2$ ha una soluzione non banale modulo p, per cui a' è un quadrato modulo p. D'altronde, se a' è un quadrato modulo p, per il lemma di Hensel-2 è anche un quadrato in $\mathbb{Q}_p$, dunque la forma $a'x^2 + b'y^2 - z^2$ ha una vettore isotropo non banale su $\mathbb{Q}_p$.

$\boxed{\alpha = \beta = 1}$ Per le proprietà del simbolo di Hilbert, ho:

$$(pa', pb') = (-p^2a'b', pb') = (-a'b', pb') = \left(\frac{-a'b'}{p}\right) = (-1)^{\frac{(p-1)}{2}} \left(\frac{a'}{p}\right)\left(\frac{b'}{p}\right).$$

Infine, per il terzo caso, devo sempre verificare solo un numero finito di casi:

$\boxed{\alpha = \beta = 0}$ Voglio dimostrare che $(a', b') = -1$ se e solo se $a' \equiv b' \equiv -1 \mod 4$. Da un lato, se la forma associata ha un vettore isotropo non banale in $\mathbb{Q}_2$, ne ha uno in $\mathbb{Z}_2$ con almeno una coordinata in $\mathbb{Z}_2^*$. Pertanto, se fosse $a' \equiv b' \equiv -1 \mod 8$, anche l'equazione $x^2+y^2+z^2 \equiv 0 \mod 4$ avrebbe una soluzione non banale, il che è assurdo. D'altronde, se almeno uno tra a' e b' (supponiamo senza perdita di generalità che sia a') è congruo a 1 modulo 4, si hanno due casi:

- se $a' \equiv 1 \mod 8$, è il quadrato di un certo $w \in \mathbb{Q}_2$ per quanto osservato alla fine della sezione 1, e $(1, 0, w)$ è un vettore isotropo della forma iniziale;
- se $a' \equiv 5 \mod 8$, si ha che $a'+4b'$ è congruo a 1 modulo 8, quindi $a'+4b'$ è il quadrato di un certo $w \in \mathbb{Q}_2$ e $(1, 2, w)$ è un vettore isotropo.

$\boxed{\alpha = 0, \beta = 1}$ Considero il caso $b' = 1$, dunque verifico che $(a', 2) = 1$ se e solo se $a' \equiv \pm 1 \mod 8$. Se $(a', 2) = 1$, per il lemma precedente esiste una soluzione all'equazione associata con $x, z \in \mathbb{Z}_2^*$, dunque $x^2 \equiv z^2 \equiv 1 \mod 8$ e $2y^2 \equiv 1 - a' \mod 8$, pertanto $a' \equiv \pm 1 \mod 8$. D'altronde, se $a' \equiv -1 \mod 8$, $(1, 1, \sqrt{a'+2})$ è una soluzione non banale, mentre se $a' \equiv 1 \mod 8$ funziona $(1, 0, \sqrt{a'})$.

Per il caso generico, dalle proprietà del simbolo di Hilbert ho che $(a', 2b') = (a', b')(a', 2)$ quando almeno uno dei due fattori al RHS è pari a 1. Se invece sono entrambi pari a -1 vuol dire che $a' \equiv b' \equiv -1 \mod 4$ e $a' \equiv \pm 3 \mod 8$, ossia $b' \equiv -1 \mod 4$ e $a' \equiv 3 \mod 8$. Ma allora $(1, 1, \sqrt{a'+2b'})$ è soluzione.

$\boxed{\alpha = \beta = 1}$ Per le proprietà del simbolo di Hilbert, ho:

$$\begin{aligned}
(2a', 2b') &= (-4a'b', 2b') \\
&= (-a'b', 2b') \\
&= (-a'b', 2)(-a'b', b') \\
&= (-a'b', 2)(a', b') \\
&= (-1)^{\frac{a'^2 b'^2 - 1}{8}} (-1)^{\frac{(a'-1)(b'-1)}{4}} \\
&= (-1)^{\frac{(a'-1)(b'-1)}{4}} (-1)^{\frac{a'^2-1}{8}} (-1)^{\frac{b'^2-1}{8}}.
\end{aligned}$$

□

Corollario 2.1.5. *Il simbolo di Hilbert $(\cdot, \cdot)_v$ è un'applicazione $\mathbb{F}_2$-bilineare simmetrica non singolare su $\mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$.*

Dimostrazione. Innanzitutto occorre osservare che $\mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$, dotato dell'operazione di prodotto, è un gruppo su cui $\mathbb{F}_2$ agisce per esponenziazione, e pertanto ha una naturale struttura di $\mathbb{F}_2$-spazio vettoriale. La bilinearità del simbolo di Hilbert è una conseguenza della moltiplicatività del simbolo di Legendre e la simmetria è ovvia. La non-singolarità va invece verificata posto per posto.

Nel caso $v = \infty$ esiste un'unica classe laterale non banale di $\mathbb{Q}_v^{*2}$, rappresentata da -1, dunque basta osservare che $(-1, -1)_\infty = -1$.

Nel caso $v = p \neq 2, \infty$, come conseguenza della proposizione 1.1.24, un insieme di rappresentanti delle classi laterali non banali di $\mathbb{Q}_p^{*2}$ è dato da $\{n, p, np\}$, dove $n \in \mathbb{Z}$ non è un quadrato

modulo p. Dalla formula si ricava che:

$$4 \nmid p-1 \Longrightarrow (pn, pn) = (n, p) = -1;$$
$$4 \mid p-1 \Longrightarrow (n, p) = (pn, n) = -1.$$

Nel caso $v = 2$, infine, sempre come conseguenza della proposizione 1.1.24, un insieme di rappresentanti delle classi laterali non banali di $\mathbb{Q}_2^{*2}$ è dato da $\{-1, 5, -5, 2, -2, 10, -10\}$, e per provare la non degenerazione basta verificare il valore del simbolo di Hilbert su tutte le combinazioni di $-1, 2, 5$, da cui si ricavano le altre per linearità. Si ha $(-1,-1) = (2,5) = -1$ e $(-1,2) = (-1,5) = (2,2) = (5,5) = 1$, dunque ad esempio:

$$(-2,5) = (-5,2) = (10,2) = (-10,2) = -1,$$

da cui la tesi. □

Lemma 2.1.6. *Se $a, b \in \mathbb{Q}_v^*/\mathbb{Q}_v^{*2} \setminus \{1\}$, $\{x|(x,a)_v = \varepsilon_a\} \cap \{x|(x,b)_v = \varepsilon_b\} = \emptyset$, allora $a = b$ e $\varepsilon_a = -\varepsilon_b$.*

Dimostrazione. I due insiemi considerati sono ciascuno una delle due classi laterali del nucleo dell'applicazione che manda x rispettivamente in $(x,a)_v$ e $(x,b)_v$, quindi, poiché il simbolo di Hilbert è non degenere, hanno entrambi cardinalità pari a $\frac{1}{2}|\mathbb{Q}_v^*/\mathbb{Q}_v^{*2}|$. Per questo motivo, se sono disgiunti devono essere complementari, e da questo, insieme alla bilinearità, segue che $\forall x \in \mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$ $(x, ab)_v = -\varepsilon_a\varepsilon_b$. Dalla non-degenerazione segue che $-\varepsilon_a\varepsilon_b = 1$, dunque si ha la tesi. □

2.2 Formula del prodotto e conseguenze

La formula generale del simbolo di Hilbert ha come conseguenza la seguente uguaglianza fondamentale.

Proposizione 2.2.1 (Formula del prodotto)**.** *Siano $a, b \in \mathbb{Q}^*$. Allora $(a,b)_v = -1$ solo per un numero finito di posti v. Inoltre vale $\prod_v (a,b)_v = 1$, con v che varia tra tutti i posti di $\mathbb{Q}$.*

Dimostrazione. Per bilinearità mi basta dimostrare il teorema nei seguenti casi (dove con p e q indicherò dei generici primi dispari):

$\boxed{a = b = -1}$ Si ha che:

$$(-1,-1)_2 = (-1)^{\frac{[(-1)-1][(-1)-1]}{4}} = -1;$$
$$(-1,-1)_\infty = -1;$$

mentre $(-1,-1)_v = 1$ in tutti gli altri posti v. Dunque:

$$\prod_v (a,b)_v = \prod_v (-1,-1)_v = (-1,-1)_2(-1,-1)_\infty.$$

$\boxed{a = -1, b = 2}$ Per le proprietà del simbolo di Hilbert, per ogni posto v vale che $(a, 1-a)_v = 1$, dunque in particolare $(-1,2)_v = 1$.

$\boxed{a=-1, b=p}$

$$\prod_v (a,b)_v = \prod_v (-1,p)_v = (-1,p)_2(-1,p)_p = (-1)^{\frac{p-1}{2}} \left(\frac{-1}{p}\right) = 1.$$

$\boxed{a=2, b=2}$

$$\prod_v (a,b)_v = \prod_v (2,2)_v = (2,2)_2 = 1.$$

$\boxed{a=2, b=p}$

$$\prod_v (a,b)_v = \prod_v (2,p)_v = (2,p)_2(2,p)_p = (-1)^{\frac{p^2-1}{8}} \left(\frac{2}{p}\right) = 1,$$

dove l'ultima uguaglianza deriva dalla formula del simbolo di Legendre $\left(\frac{2}{p}\right)$, di cui è riportata una dimostrazione nel capitolo 4.

$\boxed{a=p, b=p}$

$$\begin{aligned}\prod_v (a,b)_v &= \prod_v (p,p)_v \\ &= (p,p)_2(p,p)_p \\ &= (-1)^{\frac{(p-1)^2}{4}}(-1)^{\frac{p-1}{2}} \\ &= 1.\end{aligned}$$

$\boxed{a=p, b=q}$

$$\begin{aligned}\prod_v (a,b)_v &= \prod_v (p,q)_v \\ &= (p,q)_2(p,q)_p(p,q)_q \\ &= (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) \\ &= 1,\end{aligned}$$

dove l'ultima uguaglianza è una conseguenza della legge di reciprocità quadratica, di cui è riportata una dimostrazione nel capitolo 4.

□

L'esistenza della formula del prodotto dimostra la presenza di un vincolo "globale" al possibile valore del simbolo di Hilbert. La seguente proposizione risponde al problema inverso, provando che in un certo senso è anche l'unico vincolo.

Proposizione 2.2.2. *Sia $(a_i)_{i\leq n}$ una n-upla di numeri razionali e sia $\varepsilon_{i,v} \in \{\pm 1\}$ al variare di i tra 1 e n e di v tra i posti di $\mathbb{Q}$, tali che:*

- $\forall i\ \varepsilon_{i,v} = -1$ *al più per un numero finito di v;*
- $\prod_v \varepsilon_{i,v} = 1$*;*

- $\forall v\ \exists x_v \in \mathbb{Q}_v$ *tale che* $\forall i\ (a_i, x_v)_v = \varepsilon_{i,v}$.

Allora $\exists x \in \mathbb{Q}$ *tale che* $\forall i, v\ (a_i, x)_v = \varepsilon_{i,v}$.

Dimostrazione. Senza perdita di generalità è possibile prendere gli a_i interi e liberi da quadrati. Sia S l'insieme che contiene 2, ∞ e i fattori primi degli a_i, e sia $T := \{v|\ \exists i : \varepsilon_{v,i} = -1\}$: entrambi sono insiemi finiti per ipotesi.

Considero dapprima il caso $S \cap T = \emptyset$, e prendo

$$a := \prod_{p \in T} p;$$
$$m := 8 \prod_{p \in S \setminus \{2,\infty\}} p.$$

L'ipotesi $S \cap T = \emptyset$ implica che a e m sono coprimi, dunque, per il Teorema di Dirichlet sulle successioni aritmetiche, esiste un numero primo $q \equiv a \mod m$; affermo che $x = aq$ ha le proprietà richieste.

$\boxed{v \in S}$ Poiché $S \cap T = \emptyset$ ho che $\forall i\ \varepsilon_{i,v} = 1$. Se $v = p \neq 2, \infty$, si ha:

$$(x, a_i)_p = \left(\frac{x}{p}\right) = \left(\frac{a^2}{p}\right) = 1.$$

Nel caso $v = 2$, $(x, a_i)_2 = 1$ perché $x \equiv 1 \mod 8$, dunque è nella classe laterale banale di $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$. Infine, nel caso $v = \infty$, $(x, a_i)_\infty = 1$ perché $x > 0$.

$\boxed{v = p \in T}$ Poiché $\forall i\ p \nmid a_i$ e $2, \infty \notin T$, p deve dividere x_p, altrimenti $\forall i\ (a_i, x_p) = 1$, che è assurdo perché almeno uno degli $\varepsilon_{i,p}$ è pari a -1. Poiché p divide anche x, ho che:

$$(x, a_i)_p = \left(\frac{a_i}{p}\right) = (x_p, a_i)_p.$$

$\boxed{v = p \notin S \cup T \cup \{q\}}$ Poiché p non divide né x né alcun a_i, ed è diverso da $2, \infty$, ho che:

$$(x, a_i) = 1 = \varepsilon_{i,p}.$$

$\boxed{v = q}$ Per la formula del prodotto:

$$(x, a_i)_q = \prod_{v \neq q} (x, a_i)_v = \prod_{v \neq q} (x_v, a_i)_v = (x_q, a_i)_q.$$

Nel caso generale in cui $S \cap T \neq \emptyset$, essendo S finito, il Teorema Cinese del Resto dice che esiste $x' \in \mathbb{Q}^*$ tale che, per ogni $v \in S$, $\frac{x'}{x_v} \in \mathbb{Q}_v^{*2}$, poiché basta imporre:

$$x' \equiv_p x_p \text{ per } v = p \in S \setminus \{2, \infty\};$$
$$x' \equiv_8 x_2 \text{ nel caso } v = 2;$$
$$\frac{x'}{x_\infty} > 0 \text{ nel caso } v = \infty.$$

Pertanto:

$$\forall v \in S\ (x', a_i)_v = (x_v, a_i)_v = \varepsilon_{i,v}.$$

Prendo ora $\delta_{i,v} := (x', a_i)_v \cdot \varepsilon_{i,v}$. Questa rispetta le proprietà richieste dalle ipotesi del teorema, e inoltre per $v = 2, \infty$ o fattore primo di uno degli a_i, $\delta_{i,v} = 1$, dunque ricado nell'ipotesi semplificata ed esiste $x \in \mathbb{Q}^*$ tale che:

$$\forall i, v\ (x, a_i)_v = \delta_{i,v} = (x', a_i)_v \cdot \varepsilon_{i,v} \Longrightarrow \forall i, v\ \left(a_i, \frac{x}{x'}\right)_v = \varepsilon_{i,v}.$$

□

Proposizione 2.2.3. *Sia $q = \langle a_1, ..., a_n \rangle$ una forma quadratica non degenere in n variabili sul campo $\mathbb{Q}_p$. Definisco i due valori $d := \prod_i a_i$ e $\varepsilon = \prod_{i<j} (a_i, a_j)_p$. q rappresenta lo 0 se e solo se vale una delle seguenti (dove le congruenze sono da intendersi in $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$):*

1a $n = 2$ *e* $d \equiv -1$*;*

2a $n = 3$ *e* $(-1, -d) = \varepsilon$*;*

3a $n = 4$ *e* $d \not\equiv 1 \vee (d \equiv 1 \wedge (-1, -d) = \varepsilon)$*;*

4a $n \geq 5$.

Inoltre q rappresenta $c \in \mathbb{Q}_p^*$ se e solo se:

1b $n = 1$ *e* $c \equiv d$*;*

2b $n = 2$ *e* $(c, -d) = \varepsilon$*;*

3b $n = 3$ *e* $c \not\equiv -d \vee (c \equiv -d \wedge (-1, -d) = \varepsilon)$*;*

4b $n \geq 4$.

Dimostrazione. Gli ultimi quattro casi sono una conseguenza dei rispettivi primi quattro casi tramite manipolazione dei simboli di Hilbert e utilizzando che q rappresenta $c \in \mathbb{Q}_p^*$ se e solo se $q - cx^2$ rappresenta lo 0, pertanto è riportata la sola dimostrazione dei primi quattro casi.

1a Innanzitutto se $ax^2 + by^2 = 0$ con $(x, y) \neq (0, 0)$, sia x che y devono essere diversi da 0. Pertanto la forma $q = ax^2 + by^2$ è isotropa se e solo se esistono x_0 e y_0 tali che $-ab = \left(\frac{ax}{y}\right)^2$, ossia se e solo se $-ab$ è un quadrato. D'altronde, poiché $d = ab$, questo equivale a scrivere che $d \equiv -1$.

2a Data la forma non degenere $ax^2 + by^2 + cz^2$, posso moltiplicarla per c, che è non nullo, e ottenere una forma con gli stessi vettori isotropi: $acx^2 + bcy^2 + c^2z^2$. Usando il cambio di variabile $z' := cz$, ho che quest'ultima forma rappresenta lo 0 se e solo se esiste una soluzione non banale di $-acx^2 - bcy^2 = z'^2$, ossia se vale:

$$\begin{aligned} 1 &= (-ac, -bc) \\ &= (-1, -1)(-1, b)(-1, c)(a, -1)(a, b)(a, c)(c, -1)(c, b)(c, c) \\ &= (-1, -1)(-1, a)(-1, b)(-1, c) \cdot (a, b)(b, c)(c, a) \cdot (-1, c)(c, c) \\ &= (-1, -d)\varepsilon. \end{aligned}$$

3a La forma non degenere $q = \langle a_1, a_2, a_3, a_4 \rangle$ rappresenta lo 0 se e solo se $\exists c \in \mathbb{Q}_p$ tale che:

$$q_1 := a_1x_1^2 + a_2x_2^2 = c = -a_3x_3^2 - a_4x_4^2 =: q_2.$$

Siano A e B le classi di $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ degli elementi non nulli di $\mathbb{Q}_p$ rappresentati rispettivamente dalle forme q_1 e q_2: la forma di partenza rappresenta lo 0 se e solo se $A \cap B \neq \emptyset$. Per il caso **2b**, si ha:

$$A = \{x | (x, -a_1a_2) = (-a_1, -a_2)\}$$
$$B = \{x | (x, -a_3a_4) = (a_3, a_4)\}.$$

Per il lemma 2.1.6, $A \cap B = \emptyset$ se e solo se $-a_1a_2 = -a_3a_4$ e $(-a_1, -a_2) = -(a_3, a_4)$, oppure se uno tra A e B è vuoto, ma quest'ultimo caso è assurdo. Da $-a_1a_2 = -a_3a_4$ ricaviamo che $d = a_1a_2a_3a_4 = 1$ e che:

$$1 = (a_1a_2, -a_1a_2) = (a_3a_4, -a_1a_2) = (a_1, a_3)(a_1, a_4)(a_2, a_3)(a_2, a_4)(-1, a_3a_4).$$

Inoltre, dall'altra uguaglianza si ricava:

$$-1 = (a_3, a_4)(a_1, a_2)(-1, -a_1a_2).$$

Moltiplicando le due equazioni, si ottiene $-1 = \varepsilon(-1, -d)$. Pertanto, la forma non rappresenta lo 0 se e solo se $d \equiv 1$ e $(-1, -d) = -\varepsilon$.

4a Basta verificare la tesi per $n = 5$. Riscrivo la forma come $q = q_1 - q_2$, dove q_1 è forma di rango 2 e q_2 è una forma di rango 3, e definisco gli stessi insiemi A e B. Per il caso **2b**, A è una classe laterale del nucleo dell'applicazione che manda x in $(x, -d_1)$, ed essendo non vuoto ha cardinalità almeno $\frac{1}{2}|\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}| \geq 2$. D'altronde, per il caso **3b**, B contiene tutti gli elementi di $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ tranne al più uno, dunque $A \cap B \neq \emptyset$ e la forma rappresenta sempre lo 0.

□

Osservazione 2.2.4. Le dimostrazioni dei primi tre casi (sia a che b) funzionano anche nel caso in cui il campo in questione sia $\mathbb{R}$. Solo l'ultima dimostrazione fallisce, poiché si è usato che la cardinalità di $\mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$ è almeno 4 quando v è un numero primo, mentre nel caso $v = \infty$ è pari a 2. D'altronde, gli enunciati **4a** e **4b** sono chiaramente falsi nel caso in cui il campo di riferimento sia $\mathbb{R}$, poiché le forme con tutti i coefficienti dello stesso segno non possono mai essere isotrope sui numeri reali, indipendentemente dal rango della forma.

Caratterizzare il caso $\mathbb{Q}_v = \mathbb{R}$ può sembrare superfluo (è immediato osservare che una forma quadratica rappresenta lo 0 su $\mathbb{R}$ se e solo se ha almeno due coefficienti discordi), ma poter utilizzare le stesse formule sia quando si parla dei $\mathbb{Q}_p$ sia quando si parla di $\mathbb{R}$ è utile per ridurre i casi particolari all'interno delle dimostrazioni.

Capitolo 3

Il Teorema di Hasse-Minkowski

3.1 Enunciato e dimostrazione

Teorema 3.1.1 (Hasse-Minkowski, [Coh07, cap.5])**.** *Sia q una forma quadratica a coefficienti in $\mathbb{Q}$. Essa ammette vettori isotropi non banali in $\mathbb{Q}$ se e solo se ne ammette in $\mathbb{Q}_v$ per ogni posto v di $\mathbb{Q}$.*

Dimostrazione. Poiché se una forma ammette un vettore isotropo x su $\mathbb{Q}$, x è un vettore isotropo anche su tutti i $\mathbb{Q}_v$, basta dimostrare l'altra implicazione, ossia che, se una forma rappresenta lo 0 in ogni $\mathbb{Q}_v$, allora lo rappresenta in $\mathbb{Q}$. Inoltre, se la forma q è degenere su $\mathbb{Q}$, ammette sicuramente vettori isotropi non banali, dunque non c'è nulla da dimostrare: ci si può limitare a studiare il caso non degenere. Detto n il rango di q, in base a quanto affermato nel capitolo 2, q è equivalente ad una forma quadratica diagonale non degenere in n variabili, per cui basterà dimostrare il teorema in questo caso.

$\boxed{n=2}$ $q = ax^2 + by^2$ non degenere rappresenta lo 0 in $\mathbb{Q}_v$ se e solo se $c := -ab^{-1}$ è un quadrato in $\mathbb{Q}_v$. Se c non fosse un quadrato in $\mathbb{Q}$ avrei che o $c < 0$, dunque c non è un quadrato in $\mathbb{R}$, o $c > 0$ ed $\exists p$ tale che $2 \nmid v_p(c)$: ma allora c non è un quadrato in $\mathbb{Q}_p$, poiché $v_p(\mathbb{Q}_p^{*2}) = 2v_p(\mathbb{Q}_p) = 2\mathbb{Z}$.

$\boxed{n=3}$ Prendo $q' = a_1x_1^2 + a_2x_2^2 + a_3x_3^2$ una forma quadratica non degenere. q' è equivalente alla forma ottenuta dividendo tutti i suoi coefficienti per $-a_3$: $q'' := -\frac{a_1}{a_3}x_1^2 - \frac{a_2}{a_3}x_2^2 - x_3^2$. Chiamo $a' = -\frac{a_1}{a_3}$ e $b' = -\frac{a_1}{a_3}$. Inoltre, moltiplicando x e y per opportuni fattori, ottengo una terza forma equivalente: $ax^2 + by^2 - z^2$, con $a, b \in \mathbb{Z}$ liberi da quadrati. Senza perdita di generalità suppongo $|a| \leq |b|$ e procedo per induzione su $m := |a| + |b|$.

Se $m = 2$ si ha che o $a = b = -1$, dunque q non rappresenta lo 0 in $\mathbb{R}$, o almeno uno tra a e b è pari a 1, dunque q rappresenta lo 0 in $\mathbb{Q}$.

Se $m > 2$ ho $|b| \geq 2$, dunque posso scrivere b come $\pm p_1 \cdots p_n$, dove i p_i sono numeri primi positivi e distinti. Assumo che la forma abbia vettori isotropi in ogni $\mathbb{Q}_v$. In particolare, preso p primo che divide b, q ha un vettore isotropo in $\mathbb{Q}_p$, dunque, per il lemma 2.1.3, l'equazione $ax^2 + by^2 = z^2$ ha una soluzione non banale in $\mathbb{Z}_p$ tale che $v_p(x) = 0$.

Quozientando per $p\mathbb{Z}_p$ e ricordando che $x \not\equiv 0 \mod p$, si ha:

$$ax^2 \equiv z^2 \mod p \Longrightarrow a \equiv (zx^{-1})^2 \mod p,$$

quindi a è un quadrato modulo p. Poiché è vero per ogni primo p che divide b, per il teorema cinese del resto a è un quadrato anche modulo b, quindi esistono $k, b' \in \mathbb{Z}$ con $|2k| \leq b$ tali che $a - k^2 = bb'$. Inoltre, essendo $|a| \leq |b|$ e $|b| \geq 2$, si ha:

$$|b'| = \frac{|a - k^2|}{|b|} \leq \frac{|b| + \frac{b^2}{4}}{|b|} = \frac{|b|}{4} + 1 < |b|.$$

Noto che per ogni campo $\mathbb{K} \supseteq \mathbb{Q}$, posti $c, d \in \mathbb{K}^*$, se (u, v, w) con $u, v, w \in \mathbb{K}$ non tutti nulli è una soluzione dell'equazione $cx^2 + dy^2 = z^2$, allora o $u = 0 \wedge d \in \mathbb{K}^{*2}$ o $c = \left(\frac{w}{u}\right)^2 - d\left(\frac{v}{u}\right)^2$; denotando, quando d non è un quadrato in $\mathbb{K}^*$, $N_d := \mathcal{N}(\mathbb{K}(\sqrt{d}))$, ossia l'immagine del campo $\mathbb{K}(\sqrt{d})$ mediante la sua norma come estensione di $\mathbb{K}$, ho che quindi o d è un quadrato in $\mathbb{K}$ o $c \in N_d$. Viceversa, se d è un quadrato in $\mathbb{K}$, $\exists\, a \in \mathbb{K}$ tale che $d = a^2$, e in particolare $(0, 1, a)$ è una soluzione di $cx^2 + dy^2 = z^2$; se invece d non è un quadrato in $\mathbb{K}$ e $c \in N_d$, allora si può scrivere c come $a^2 - db^2$, con $a, b \in \mathbb{K}$, e in particolare $(1, b, a)$ è una soluzione di $cx^2 + dy^2 = z^2$.

Detta $q' := ax^2 + b'y^2 - z^2$, ho che, per ogni campo di numeri $\mathbb{K}$, se $a \in \mathbb{K}^{*2}$, allora sia q che q' rappresentano lo 0 in $\mathbb{K}$. Nel caso in cui $a \notin \mathbb{K}^{*2}$, q rappresenta lo 0 in $\mathbb{K}$ se e solo se $b \in N_a$. Poiché N_a è un gruppo e $bb' \in N_a$, ho $b \in N_a$ se e solo se $b' \in N_a$, che a sua volta avviene se e solo se q' rappresenta lo 0 su $\mathbb{K}$. Da questi due casi, si ottiene che poiché q è isotropa su ogni campo locale $\mathbb{Q}_v$, lo è anche q'. Tuttavia, poiché $|a| + |b'| < m$, l'ipotesi induttiva mi dice q' è isotropa anche su $\mathbb{Q}$, perciò anche q è isotropa su $\mathbb{Q}$.

$n = 4$ $\langle a_1, a_2, a_3, a_4 \rangle$ è isotropa su $\mathbb{Q}_v$ se e solo se $\exists c_v \in \mathbb{Q}_v$ tale che $a_1 t_1^2 + a_2 t_2^2 = c_v = -a_3 t_3^2 - a_4 t_4^2$ per qualche quaterna (t_1, t_2, t_3, t_4) di elementi di $\mathbb{Q}_v$. Questo è equivalente a dire che $\exists c_v \in \mathbb{Q}_v$ tale che le forme quadratiche $a_1 x_1^2 + a_2 x_2^2$ e $-a_3 x_3^2 - a_4 x_4^2$ rappresentano entrambe c_v. Inoltre posso supporre $c_v \neq 0$, poiché se una forma rappresenta lo 0 può rappresentare ogni numero del campo per il lemma 1.2.4. Infine, per la proposizione 2.2.3, la forma quadratica non degenere in 2 variabili $ax^2 + by^2$ rappresenta c se e solo se $(a, b) = (-ab, c)$. Le ipotesi sono dunque equivalenti a:

$$\forall v\ \exists c_v \in \mathbb{Q}_v \text{ tale che } (a_1, a_2)_v = (-a_1 a_2, c_v)_v \text{ e } (-a_3, -a_4)_v = (-a_3 a_4, c_v)_v.$$

Posso ora applicare la proposizione 2.2.2. Infatti, presi i due numeri razionali $-a_1 a_2$ e $-a_3 a_4$ ho che:

- $(a_1, a_2)_v$ e $(-a_3, -a_4)_v$ sono pari a $= -1$ al più per un numero finito di v;
- $\prod_v (a_1, a_2)_v = 1$ e $\prod_v (-a_3, -a_4)_v = 1$ grazie alla formula del prodotto del simbolo di Hilbert;
- $\forall v\ \exists c_v \in \mathbb{Q}_v$ tale che $(a_1, a_2)_v = (-a_1 a_2, c_v)_v$ e $(-a_3, -a_4)_v = (-a_3 a_4, c_v)_v$.

Pertanto, esiste $c \in \mathbb{Q}$ tale che:

$$(a_1, a_2)_v = (-a_1 a_2, c)_v \text{ e } (-a_3, -a_4)_v = (-a_3 a_4, c)_v,$$

che è equivalente a dire che le forme $\langle a_1, a_2, -c \rangle$ e $\langle -a_3, -a_4, -c \rangle$ rappresentano entrambe lo 0 in ogni $\mathbb{Q}_v$. Ciò, per il caso in 3 variabili del teorema, implica che entrambe le forme rappresentano lo 0 in $\mathbb{Q}$, che è equivalente a dire che $a_1 x_1^2 + a_2 x^2$ e $-a_3 x_3^2 - a_4 x_4^2$ rappresentano c in $\mathbb{Q}$, dunque la loro differenza q rappresenta lo 0.

$\boxed{n=5}$ In questo caso, posso scrivere la forma quadratica come $q_1 - q_2$, dove q_1 è una forma di rango 2 e q_2 di rango 3. Dalla proposizione 2.2.3 si ha che q_2 rappresenta lo 0 su $\mathbb{Q}_v$ se $(-1,-d_2)_v = \varepsilon_2$ (con ovvio significato di d_2 e ε_2): dalla formula del simbolo di Hilbert, ciò avviene per ogni $v \neq 2,\infty$ che non divida i coefficienti di q_2. In particolare, ciò vuol dire che a meno di un insieme finito di posti S, q_2 rappresenta tutti gli elementi di $\mathbb{Q}_v$. D'altronde, per ogni $v \in S$, esiste un $c_v \in \mathbb{Q}_v^*$ rappresentato sia da q_1 che da q_2. Considero l'insieme $c_v\mathbb{Q}_v^{*2} \subseteq \mathbb{Q}_v$: questo è aperto rispetto alla norma $\|\cdot\|_v$ perché classe laterale dell'insieme aperto $\mathbb{Q}_v^{*2}$ (il fatto che quest'ultimo sia aperto è una conseguenza della sua struttura, mostrata per $v \neq \infty$ nella proposizione 1.1.24). Poiché q_1 è un polinomio, è continuo rispetto ad ogni norma $\|\cdot\|_v$, dunque $\forall v \in S$ la controimmagine $A_v = q_1^{-1}\left(c_v\mathbb{Q}_v^{*2}\right)$ è un sottoinsieme aperto di $\mathbb{Q}_v \times \mathbb{Q}_v$. Per il lemma di approssimazione (proposizione 1.1.18), poiché S è finito, esiste una coppia $(x,y) \in \mathbb{Q}\times\mathbb{Q}$ che appartiene ad A_v per ogni $v \in S$, dunque $a := q_1(x,y)$ è un numero razionale che appartiene a $c_v\mathbb{Q}_v^{*2}$ per ogni $v \in S$. Questo vuol dire che la forma $q_2 - at^2$ è isotropa su ogni $\mathbb{Q}_v$ con $v \in S$, per la costruzione appena effettuata, ed è isotropa anche su ogni $\mathbb{Q}_v$ con $v \notin S$ perché lo è q_2. Dunque, per il caso precedente del teorema, $q_2 - at^2$ è isotropa anche su $\mathbb{Q}$; ma poiché anche $q_1 - at^2$ è isotropa su $\mathbb{Q}$ per definizione di a, la forma $q_1 - q_2$ è isotropa su $\mathbb{Q}$.

$\boxed{n>5}$ La forma q è isotropa su $\mathbb{R}$, dunque due suoi coefficienti sono discordi. Scrivo la forma quadratica come $q = q_1 + q_2$, dove q_1 è una forma di rango 5 e q_2 di rango $n-5$, in modo che q_1 contenga i termini con i coefficienti discordi di q, e pertanto q_1 è isotropa su $\mathbb{R}$. Inoltre, q_1 è isotropa su tutti i $\mathbb{Q}_p$ per la proposizione 2.2.3, quindi per il caso precedente del teorema è isotropa su $\mathbb{Q}$, e dunque a maggior ragione anche q è isotropa su $\mathbb{Q}$.

□

3.2 Conseguenze ed esempi

Una prima essenziale conseguenza del teorema di Hasse-Minkowski è la seguente:

Corollario 3.2.1. *Ogni forma quadratica razionale di rango $n \geq 5$ ammette vettori isotropi su $\mathbb{Q}$ se e solo se ne ammette su $\mathbb{R}$.*

Dimostrazione. Questo risultato è una diretta conseguenza del fatto che per la proposizione 2.2.3 tutte le forme quadratiche di rango $n \geq 5$ sono isotrope su tutti i campi p-adici. □

Si riporta ora il seguente lemma dovuto a Gauss, di cui si può trovare una dimostrazione in [Gre83]:

Lemma 3.2.2. *Se un numero intero è ottenuto come somma di n quadrati razionali, con $n = 3, 4$, allora si può scrivere come somma di n quadrati interi.*

Sfruttando questo risultato, il teorema di Hasse-Minkowski ha come conseguenza i seguenti teoremi.

Teorema 3.2.3 (Teorema dei 4 quadrati)**.** *Ogni numero intero positivo n si può scrivere come somma di 4 quadrati interi.*

Dimostrazione. Per il lemma di Gauss, basta dimostrare che n si scrive come somma di 4 quadrati razionali, ossia che la forma $\langle 1,1,1,1,-n\rangle$ è isotropa su $\mathbb{Q}$. Tuttavia, avendo rango 5 è isotropa su tutti i campi p-adici, e poiché non tutti i suoi coefficienti hanno segno concorde è isotropa anche su $\mathbb{R}$. Per il teorema di Hasse-Minkowski, deve dunque essere isotropa anche su $\mathbb{Q}$. □

Teorema 3.2.4 (Teorema dei 3 quadrati)**.** *Ogni numero intero positivo n si può scrivere come somma di 3 quadrati interi se e solo se n non si scrive come $4^a(8b+7)$, dove a, b sono numeri naturali.*

Dimostrazione. Per il lemma di Gauss, n è la somma di 3 quadrati interi se e solo se è la somma di 3 quadrati razionali, dunque se e solo se la forma $q = \langle 1, 1, 1, -n\rangle$ è isotropa su $\mathbb{Q}$. Per il teorema di Hasse-Minkowski, ciò avviene se e solo se q è isotropa su ogni $\mathbb{Q}_v$. q è isotropa su $\mathbb{R}$ perché possiede almeno due coefficienti discordi. Sui restanti $\mathbb{Q}_p$, per la proposizione 2.2.3, q è isotropa se e solo se d non è un quadrato in $\mathbb{Q}_p$ oppure d è un quadrato e $(-1,-1)_p = \varepsilon$, dove $d = -n$ e $\varepsilon = (1,1)_p(1,1)_p(1,1)_p(1,-n)_p(1,-n)_p(1,-n)_p = 1$. Pertanto, la seconda condizione si riscrive come $(-1,-1)_p = 1$, che, per la formula del simbolo di Hilbert, è verificata per ogni $p \neq 2$. Da ciò si ha che q è isotropa su $\mathbb{Q}$ se e solo se è isotropa su $\mathbb{Q}_2$. Per $p = 2$ si ha che $(-1,-1)_p = -1$, pertanto q è isotropa se e solo se $-n$ non è un quadrato in $\mathbb{Q}_2$. Per la proposizione 1.1.12, ciò avviene se e solo se $v_2(-n)$ è pari e $\frac{-n}{2^{v_2(-n)}} \equiv_8 1$. Da questo si deduce che n si scrive come $4^a c$ con c dispari e che $-c \equiv_8 1$, ossia $c \equiv_8 7$.

Ricapitolando, n si scrive come somma di 3 quadrati interi se e solo se $n \neq 4^a(8b+7)$, come volevasi dimostrare. □

Un ulteriore risultato, che sfrutta la formula del prodotto del simbolo di Hilbert, è il seguente raffinamento del teorema di Hasse-Minkowski.

Teorema 3.2.5. *Sia q una forma quadratica a coefficienti razionali di rango n pari a 2 o 3 e si fissi un campo locale $\mathbb{Q}_w$. Se q ammette vettori isotropi su ogni campo locale eccetto $\mathbb{Q}_w$, allora ne ammette su $\mathbb{Q}$ (e dunque anche su $\mathbb{Q}_w$).*

Dimostrazione. Come nel teorema di Hasse-Minkowski, assumeremo senza perdita di generalità che la forma q sia scritta in forma diagonale.

$\boxed{n=2}$ $q = ax^2 + by^2$ è isotropa su $\mathbb{Q}_v$ se e solo se $\frac{-b}{a}$ è un quadrato in $\mathbb{Q}_v$. In particolare, per ogni $x \in \mathbb{Q}$ vale che $\left(\frac{-b}{a}, x\right)_v = 1$ per ogni posto $v \neq w$. Dalla formula del prodotto si ricava che:

$$\left(\frac{-b}{a}, x\right)_w = \prod_{v \neq w} \left(\frac{-b}{a}, x\right)_v = 1.$$

Se per assurdo $\frac{-b}{a}$ non fosse un quadrato su $\mathbb{Q}_w$, poiché il simbolo di Hilbert è non degenere, esisterebbe una classe laterale di $c\mathbb{Q}_w^{*\,2}$ tale che $\forall y \in c\mathbb{Q}_w^{*\,2}$ vale che $\left(\frac{-b}{a}, y\right)_w = -1$. Tuttavia ogni classe laterale di $\mathbb{Q}_w^{*\,2}$ è topologicamente aperta in $\mathbb{Q}_w$, e poiché quest'ultimo è il completamento dei numeri razionali, $\mathbb{Q}$ è denso in $\mathbb{Q}_w$, e in particolare $\mathbb{Q} \cap c\mathbb{Q}_w^{*\,2} \neq \emptyset$. Prendendo dunque y in questa intersezione, si ha $\left(\frac{-b}{a}, y\right)_w = -1$; che è assurdo perché contrario a quanto dedotto dalla formula del prodotto. Pertanto q è isotropa su tutti i $\mathbb{Q}_v$, e dunque è isotropa su $\mathbb{Q}$ per il teorema di Hasse-Minkowski.

$\boxed{n=3}$ Per la proposizione 2.2.3, $q = ax^2 + by^2 + cz^2$ è isotropa su $\mathbb{Q}_v$ se e solo se $(-1,-d)_v = \varepsilon$, ossia se $(-1,-abc)_v = (a,b)_v(b,c)_v(c,a)_v$. Poiché quest'uguaglianza vale per ogni posto $v \neq w$, dalla formula del prodotto si ha:

$$(-1,-abc)_w = \prod_{v \neq w} (-1,-abc)_v = \prod_{v \neq w} (a,b)_v(b,c)_v(c,a)_v = (a,b)_w(b,c)_w(c,a)_w.$$

Pertanto q è isotropa anche su $\mathbb{Q}_w$, e dunque è isotropa su $\mathbb{Q}$ per il teorema di Hasse-Minkowski. □

Osservazione 3.2.6. Per quanto riguarda i casi in cui $n \geq 5$, è facile constatare che il teorema 3.2.5 non può valere: infatti, ogni forma quadratica diagonale di rango n con tutti i coefficienti di segno concorde è isotropa su ogni $\mathbb{Q}_p$ per la proposizione 2.2.3, ma non può essere isotropa su $\mathbb{R}$. Un controesempio per $n = 4$ si può dedurre dalla dimostrazione del teorema 3.2.4: se $n = 4^a(8b + 7)$ con $a, b \in \mathbb{N}$, la forma $\langle 1, 1, 1, -n \rangle$ è isotropa su $\mathbb{R}$ e su tutti i $\mathbb{Q}_p$ per $p \neq 2$, ma non è isotropa su $\mathbb{Q}_2$.

Capitolo 4

Reciprocità quadratica e cubica

Di seguito si riporta la dimostrazione delle leggi di reciprocità quadratica e cubica. Per approfondimenti, si rimanda a [IR90].

4.1 Somme di Gauss e somme di Jacobi

Definizione 4.1.1. Dato un numero primo naturale p, si dice *carattere* di $\mathbb{F}_p^*$ un qualsiasi omomorfismo di gruppi χ tra $(\mathbb{F}_p^*, \cdot)$ e $(\mathbb{C}^*, \cdot)$. In particolare, χ ha immagine nelle radici $p-1$ esime complesse dell'unità. Il carattere che vale costantemente 1 viene detto carattere banale ed è indicato con χ_{triv}.

Durante la dimostrazione si considereranno i caratteri di $\mathbb{F}_p^*$ come funzioni definite su tutto $\mathbb{F}_p$. In tal caso, si prenderà $\chi(0) = 0$.

Definizione 4.1.2. Dato un primo naturale p e un elemento $a \in \mathbb{F}_p$, e posta ζ_p una radice p-esima dell'unità, una *somma di Gauss* è una funzione che associa ad un carattere di $\mathbb{F}_p^*$ il numero complesso:

$$g_a(\chi) = \sum_{x \in \mathbb{F}_p} \chi(x)\zeta_p^{ax}.$$

Per semplicità di notazione, la somma di Gauss g_1 sarà indicata con la sola g.

Definizione 4.1.3. Dato un primo naturale p, la *somma di Jacobi* relativa ai caratteri χ_1 e χ_2 di $\mathbb{F}_p^*$, è il numero complesso:

$$J(\chi_1, \chi_2) = \sum_{x \in \mathbb{F}_p} \chi_1(x)\chi_2(1-x).$$

Proposizione 4.1.4. *Valgono le seguenti relazioni:*

- *se* $a \neq 0$, $g_a(\chi) = \overline{\chi}(a)g(\chi)$, *mentre* $g_0(\chi) = 0$ *se* $\chi \neq \chi_{triv}$;
- $|g(\chi)|^2 = g(\chi)\overline{g(\chi)} = p$;
- $g(\overline{\chi}) = \overline{\chi}(-1)\overline{g(\chi)}$;
- *Se* $\chi_2 \neq \overline{\chi_1}$, *si ha* $g(\chi_1)g(\chi_2) = J(\chi_1, \chi_2)g(\chi_1\chi_2)$.

Dimostrazione.

- Preso un generatore h di $\mathbb{F}_p^*$, si ha che ogni elemento di $\mathbb{F}_p^*$ si scrive in modo unico come h^n, con n che va da 0 a $p-2$. Poiché $\chi(h^n) = \chi(h)^n$, $\chi = \chi_{triv}$ se e solo se $\chi(h) = 1$, quindi:

$$g_0(\chi) = \sum_{x \in \mathbb{F}_p} \chi(x) = \sum_{i=0}^{p-2} \chi(h)^i = \frac{1 - \chi(h)^{p-1}}{1 - \chi(h)} = 0.$$

  Se invece $a \neq 0$:

$$g_a(\chi) = \sum_{x \in \mathbb{F}_p} \chi(x)\zeta_p^{ax} = \chi a^{-1} \sum_{x \in \mathbb{F}_p} \chi(ax)\zeta_p^{ax} = \chi a^{-1} \sum_{x \in \mathbb{F}_p} \chi(x)\zeta_p^{x} = \overline{\chi}(a) g(\chi).$$

- Vale la seguente catena di uguaglianze:

$$\begin{aligned}
|g(\chi)|^2 &= g(\chi)\overline{g(\chi)} \\
&= \left(\sum_{x \in \mathbb{F}_p^*} \chi(x)\zeta_p^x \right) \left(\sum_{y \in \mathbb{F}_p^*} \overline{\chi}(y)\zeta_p^{-y} \right) \\
&= \sum_{x,y \in \mathbb{F}_p^*} \chi(x)\overline{\chi}(y)\zeta_p^{x-y} \\
&= \sum_{x,z \in \mathbb{F}_p^*} \chi(x)\overline{\chi}(xz)\zeta_p^{x-xz} \\
&= \sum_{x,z \in \mathbb{F}_p^*} \chi\overline{\chi}(x)\overline{\chi}(z)\zeta_p^{x(1-z)} \\
&= \sum_{z \in \mathbb{F}_p^*} \overline{\chi}(z) \left(\sum_{x \in \mathbb{F}_p^*} \zeta_p^{x(1-z)} \right) \\
&= \overline{\chi}(1) \left(\sum_{x \in \mathbb{F}_p^*} 1 \right) + \sum_{z \in \mathbb{F}_p^* \setminus \{1\}} \overline{\chi}(z) \left(\sum_{x \in \mathbb{F}_p^*} \left(\zeta_p^{1-z}\right)^x \right) \\
&= p - 1 + \sum_{z \in \mathbb{F}_p^* \setminus \{1\}} \overline{\chi}(z)(-1) \\
&= p - 1 + \overline{\chi}(1) - \sum_{z \in \mathbb{F}_p^*} \overline{\chi}(z) \\
&= p,
\end{aligned}$$

  dove si è utilizzato che per ogni carattere χ, il carattere prodotto $\chi\overline{\chi} = \chi_{triv}$, e che, poiché $\overline{\chi}$ non è banale, la somma su z di $\overline{\chi}(z)$ è nulla.

- Vale la seguente catena di uguaglianze:

$$g(\overline{\chi}) = \sum_{y \in \mathbb{F}_p^*} \overline{\chi}(y)\zeta_p^y = \sum_{y \in \mathbb{F}_p^*} \overline{\chi}(-y)\zeta_p^{-y} = \overline{\chi}(-1)\overline{\sum_{y \in \mathbb{F}_p^*} \chi(y)\zeta_p^y} = \overline{\chi}(-1)\overline{g(\chi)}.$$

- Vale la seguente catena di uguaglianze:

$$\begin{aligned}
g(\chi_1)g(\chi_2) &= \left(\sum_{x\in\mathbb{F}_p}\chi_1(x)\zeta_p^x\right)\left(\sum_{y\in\mathbb{F}_p}\chi_2(y)\zeta_p^y\right)\\
&= \sum_{x,y\in\mathbb{F}_p}\chi_1(x)\chi_2(y)\zeta_p^{x+y}\\
&= \sum_{x,t\in\mathbb{F}_p}\chi_1(x)\chi_2(t-x)\zeta_p^t\\
&= \sum_{x,t\in\mathbb{F}_p^*}\chi_1(x)\chi_2(t-x)\zeta_p^t + \sum_{x\in\mathbb{F}_p^*}\chi_1(x)\chi_2(-x)\\
&= \sum_{y,t\in\mathbb{F}_p^*}\chi_1(ty)\chi_2(t-ty)\zeta_p^t + \chi_2(-1)\left(\sum_{x\in\mathbb{F}_p^*}\chi_1\chi_2(x)\right)\\
&= \sum_{y,t\in\mathbb{F}_p^*}\chi_1(t)\chi_1(y)\chi_2(t)\chi_2(1-y)\zeta_p^t\\
&= \left(\sum_{y\in\mathbb{F}_p^*}\chi_1(y)\chi_2(1-y)\right)\left(\sum_{t\in\mathbb{F}_p^*}\chi_1\chi_2(t)\zeta_p^t\right)\\
&= J(\chi_1,\chi_2)g(\chi_1\chi_2).
\end{aligned}$$

□

Con queste proprietà è possibile procedere con le dimostrazioni.

4.2 Reciprocità quadratica

Definizione 4.2.1 (Simbolo di Legendre)**.** Dati un numero primo $p \in \mathbb{Z}$ e un generico numero intero a, il *simbolo di Legendre* $\left(\frac{a}{p}\right)$ è definito come segue:

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{se } p \nmid a \text{ e } a \text{ è un quadrato modulo } p \\ -1 & \text{se } p \nmid a \text{ e } a \text{ non è un quadrato modulo } p \\ 0 & \text{se } p \mid a \end{cases}.$$

Osservazione 4.2.2. Il simbolo di Legendre $\left(\frac{\cdot}{p}\right)$ è moltiplicativo; in particolare, può essere pensato come un carattere di $\mathbb{F}_p^*$.

Proposizione 4.2.3 (Legge di reciprocità quadratica)**.** *Dati $p, q \in \mathbb{Z}$ primi dispari distinti, vale che:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Inoltre, vale che:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Dimostrazione. Vale la seguente formula:

$$\overline{g(\chi)} = \sum_{x \in \mathbb{F}_p} \overline{\chi}(x)\zeta_p^{-x} = g_{-1}(\overline{\chi}) = \overline{\chi}(-1)g(\overline{\chi}).$$

Fisso un certo primo dispari p e prendo come carattere il simbolo di Legendre: $\chi(\cdot) := \left(\frac{\cdot}{p}\right)$. Per questo carattere, vale che $\overline{\chi} = \chi$, dunque:

$$p = |g(\chi)|^2 = g(\chi)\overline{g(\chi)} = g(\chi)\overline{\chi}(-1)g(\overline{\chi}) = \chi(-1)g(\chi)^2.$$

Posso considerare questa somma di Gauss a valori nell'anello $\mathbb{Z}[\zeta_p]$. Detto q un qualsiasi primo dispari diverso da p, lavoro modulo q e ho:

$$g(\chi)^q = \left(\sum_{x \in \mathbb{F}_p^*} \chi(x)\zeta_p^x\right)^q = \sum_{x \in \mathbb{F}_p^*} \chi(x)^q \zeta_p^{xq} = \overline{\chi}(q) \sum_{x \in \mathbb{F}_p^*} \chi(xq)\zeta_p^{xq} = \chi(q)g(\chi).$$

Pertanto, ottengo:

$$\left(\frac{p}{q}\right) = p^{\frac{q-1}{2}} = \left(\chi(-1)g(\chi)^2\right)^{\frac{q-1}{2}} = \chi(-1)^{\frac{q-1}{2}} g(\chi)^{q-1} = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right).$$

Questa è un'uguaglianza modulo q, ma poiché ambo i lati dell'equazione possono valere solo 1 o -1, le due espressioni coincidono su $\mathbb{Z}$.

Per quanto riguarda il valore di $\left(\frac{2}{p}\right)$, con p numero primo dispari, considero il seguente valore su $\mathbb{Z}[\zeta_8]$, dove ζ_8 è una radice primitiva ottava dell'unità: $g_2 := \zeta_8 + \zeta_8^{-1}$. Modulo p, valgono le seguenti equazioni:

$$\begin{aligned} g_2^2 &= \zeta_8^2 + \zeta_8^{-2} + 2 = \zeta_8^{-2}(\zeta_8^4 + 1) + 2 = 2 \\ g_2^p &= \zeta_8^p + \zeta_8^{-p} = \begin{cases} \zeta_8 + \zeta_8^{-1} = g_2 & \text{se } p \equiv \pm 1 \mod 8 \\ \zeta_8^3 + \zeta_8^{-3} = -\zeta_8 - \zeta_8^{-1} = -g_2 & \text{se } p \equiv \pm 3 \mod 8 \end{cases}. \end{aligned}$$

In particolare, la seconda equazione si può riscrivere come $g_2^{p-1} = (-1)^{\frac{p^2-1}{8}}$. Dunque si ha:

$$\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} = (g_2^2)^{\frac{p-1}{2}} = g_2^{p-1} = (-1)^{\frac{p^2-1}{8}}.$$

Questa è un'uguaglianza modulo p, ma poiché ambo i lati dell'equazione possono valere solo 1 o -1, le due espressioni coincidono su $\mathbb{Z}$. □

4.3 Reciprocità cubica

Proposizione 4.3.1. *Detta ζ_3 una radice cubica primitiva dell'unità, l'anello $\mathbb{Z}[\zeta_3]$, i cui elementi sono detti interi di Eisenstein, è un dominio euclideo rispetto alla norma $\mathcal{N}(x) = x\overline{x}$; in particolare, è un dominio a fattorizzazione unica. Questo anello contiene* 6 *elementi di norma* 1*, detti unità, che sono: $\pm 1, \pm\zeta_3, \pm\zeta_3^2$.*

Poiché la fattorizzazione è unica a meno di moltiplicazione per le unità, è naturale definire la seguente relazione di equivalenza.

Definizione 4.3.2. Due interi di Eisenstein a e b si dicono *associati* se esiste un'unità u tale che $a = ub$, e si scrive $a \sim b$.

A meno di associati, i numeri primi di Eisenstein sono facili da classificare. In particolare, vale la seguente proposizione:

Proposizione 4.3.3. *Dato p primo di $\mathbb{Z}$, sono possibili tre casi:*

- *se $p = 3$, si ha $3 = -(1 + 2\zeta_3)^2$, dove $1 + 2\zeta_3$ è un primo di Eisenstein;*
- *se $p \equiv_3 1$, si ha $p = \pi\overline{\pi}$, dove π e $\overline{\pi}$ sono primi di Eisenstein;*
- *se $p \equiv_3 2$, p è un primo di Eisenstein.*

In particolare, per ogni primo di Eisenstein π non associato a $1 + 2\zeta_3$ si ha che $\mathcal{N}(\pi) - 1$ è un multiplo di 3.

Nel resto della sezione, un primo denominato π indicherà sempre un numero primo di Eisenstein. Inoltre, se $\pi \in \mathbb{Z}$ verrà detto *primo razionale*, mentre se ha una componente immaginaria diversa da 0 verrà detto *primo complesso*. Per i numeri primi di Eisenstein vale una generalizzazione del piccolo teorema di Fermat:

Proposizione 4.3.4. *Sia π primo e α un intero di Eisenstein coprimo con π. Allora vale la seguente formula:*

$$\alpha^{\mathcal{N}(\pi)-1} \equiv 1 \mod \pi.$$

Avendo introdotto il concetto di primo associato, e volendo considerare i primi di Eisenstein a meno di questa relazione di equivalenza, è utile trovare una rappresentante "canonico" per ogni primo.

Definizione 4.3.5. Un primo π si dice *primario* se è congruo a 2 modulo 3.

Proposizione 4.3.6. *Se π è un primo diverso da $(1 + 2\zeta_3)$ o da uno dei suoi associati, esiste un associato di π che è primario.*

Dimostrazione. Se $\pi \sim q$, dove q è un primo di $\mathbb{Z}$, allora deve valere $q \equiv 2 \mod 3$.

Altrimenti, $\pi = a+b\zeta_3$, dove $p = \pi\overline{\pi} = a^2-ab+b^2 \equiv 1 \mod 3$ è un primo di $\mathbb{Z}$. In particolare vale $1 \equiv_3 (a^2 - ab + b^2) + 3ab = (a + b)^2$, dunque $a + b \not\equiv 0 \mod 3$. Gli associati di π sono: $\pm(a + b\zeta_3), \pm(-b + (a - b)\zeta_3), \pm((b - a) - a\zeta_3)$. Poiché $a + b \not\equiv 0 \mod 3$, uno tra b, $a - b$ e $-a$ è congruo a 0 modulo 3, di conseguenza esiste un associato di π, che denomino $u\pi$, congruo ad un numero intero modulo 3. Poiché π e i suoi associati sono coprimi con 3, questo numero è diverso da 0: da questo si ricava che uno tra $u\pi$ e $-u\pi$ è congruo a 2 modulo 3. □

Per ogni π primo non associato a $1 + 2\zeta_3$, considero il residuo modulo π di $\alpha^{\frac{\mathcal{N}(\pi)-1}{3}}$, e chiamo β un suo rappresentante. Come osservato precedentemente, per tutti i primi considerati la quantità $\mathcal{N}(\pi) - 1$ è effettivamente divisibile per 3. Inoltre, per come è stato definito si ha che $\beta^3 = \alpha^{\mathcal{N}(\pi)-1}$, dunque β è congruo a una radice cubica dell'unità (e a una sola, poiché sono tutte distinte modulo π). Per questo motivo, posso dare la seguente definizione:

Definizione 4.3.7. Per ogni primo π e per ogni intero di Eisenstein α coprimo con π, definisco il *carattere cubico* $\chi_\pi(\alpha)$ come l'unica radice cubica dell'unità congrua ad $\alpha^{\frac{\mathcal{N}(\pi)-1}{3}}$ modulo π.

Osservazione 4.3.8. Dalla definizione è chiaro che il carattere cubico è moltiplicativo.

Il nome di questo carattere deriva dal fatto che, analogamente al simbolo di Legendre per i quadrati, $\chi_\pi(\alpha) = 1$ se e solo se α è un cubo modulo π.

Si può pensare il carattere cubico definito sul campo residuo $\mathbb{Z}[\zeta_3]/\pi\mathbb{Z}[\zeta_3]$. In tal caso si assume che $\chi_\pi(0) = 0$.

Infine, se π è tale che $\mathcal{N}(\pi) = p$ è un primo di $\mathbb{Z}$ congruo a 1 modulo 3, i numeri interi da 0 a $p-1$ sono una classe di rappresentanti di $\mathbb{Z}[\zeta_3]/\pi\mathbb{Z}[\zeta_3]$: questo induce un isomorfismo canonico tra $\mathbb{Z}[\zeta_3]/\pi\mathbb{Z}[\zeta_3]$ e il campo $\mathbb{F}_p$, dunque ha senso considerare le somme di Gauss e Jacobi relative al carattere cubico.

Proposizione 4.3.9. *Sia π un primo tale che $\mathcal{N}(\pi) = p$ è un primo di $\mathbb{Z}$ congruo a 1 modulo 3 (in particolare, p è un primo dispari). Sfruttando le proprietà già dimostrate delle somme di Gauss e Jacobi, si ha la seguente: $g(\chi_\pi)^3 = pJ(\chi_\pi, \chi_\pi)$.*

Dimostrazione. Poiché $\chi_\pi^3 = \chi_{triv}$, e dunque $\chi_\pi^2 = \chi_\pi^{-1} = \overline{\chi_\pi}$, si ha:

$$\begin{aligned} g(\chi_\pi)^3 &= g(\chi_\pi)g(\chi_\pi)^2 \\ &= g(\chi_\pi)J(\chi_\pi, \chi_\pi)g(\chi_\pi^2) \\ &= J(\chi_\pi, \chi_\pi)g(\chi_\pi)g(\overline{\chi_\pi}) \\ &= J(\chi_\pi, \chi_\pi)g(\chi_\pi)\overline{g(\chi_\pi)}\overline{\chi}(-1) \\ &= pJ(\chi_\pi, \chi_\pi), \end{aligned}$$

dove nell'ultimo passaggio si è usato che $\overline{\chi}(-1) \equiv (-1)^{\frac{p-1}{3}} \equiv 1 \mod p$. □

Corollario 4.3.10. *$J(\chi_\pi, \chi_\pi)$ è primario.*

Dimostrazione. Modulo 3, si ha:

$$pJ(\chi_\pi, \chi_\pi) = g(\chi_\pi)^3 = \left(\sum_{x\in\mathbb{F}_p} \chi_\pi(x)\zeta_p^x\right)^3 \equiv \sum_{x\in\mathbb{F}_p} \chi_\pi^3(x)\zeta_p^{3x} \equiv \sum_{x\in\mathbb{F}_p^*} \zeta_p^{3x} \equiv \sum_{x\in\mathbb{F}_p^*} \zeta_p^x \equiv -1 \mod 3.$$

Poiché $p \equiv 1 \mod 3$, segue che $J(\chi_\pi, \chi_\pi) \equiv 2 \mod 3$. □

Poiché $|g(\chi_\pi)|^2 = p$, dalla formula si ricava che anche $|J(\chi_\pi, \chi_\pi)|^2 = p$, dunque $J(\chi_\pi, \chi_\pi)$ è un primo di norma p, ed è pertanto associato ad uno tra π e $\overline{\pi}$.

Proposizione 4.3.11. *π divide $J(\chi_\pi, \chi_\pi)$. Di conseguenza, essendo quest'ultimo un numero primo, $J(\chi_\pi, \chi_\pi)$ è associato a π.*

Dimostrazione. Basta valutare $J(\chi_\pi, \chi_\pi)$ modulo π:

$$J(\chi_\pi, \chi_\pi) = \sum_{x\in\mathbb{F}_p} \chi_\pi(x)\chi_\pi(1-x) \equiv \sum_{x\in\mathbb{F}_p} [x(1-x)]^{\frac{p-1}{3}} \mod \pi.$$

Tuttavia per ogni a compreso tra 1 e $p-1$, detto g un generatore di $\mathbb{F}_p^*$, si ha che $g^a \neq 1$, dunque:

$$\sum_{x\in\mathbb{F}_p} x^a = \sum_{n=0}^{p-2} g^{na} = \frac{1-g^{(p-1)a}}{1-g^a} = 0,$$

dove le uguaglianze sono da intendersi su $\mathbb{F}_p$. Poiché $[x(1-x)]^{\frac{p-1}{3}}$ è un polinomio di grado strettamente minore di $p-1$, la somma al variare di $x \in \mathbb{F}_p$ sarà pari a 0. Ne consegue che $\pi \mid J(\chi_\pi, \chi_\pi)$. □

Dalle proposizioni precedenti segue che $J(\chi_\pi, \chi_\pi)$ è l'unico associato primario di π. Nel resto della sezione, considererò π primario, dunque $J(\chi_\pi, \chi_\pi) = \pi$ e $g(\chi_\pi)^3 = \pi^2\overline{\pi}$.

Proposizione 4.3.12 (Legge di reciprocità cubica)**.** *Siano π, ρ primi primari distinti. Vale che $\chi_\pi(\rho) = \chi_\rho(\pi)$.*

Dimostrazione. Se π e ρ sono entrambi primi razionali, i caratteri cubici ad essi relativi sono banali, dunque $\chi_\pi(\rho) = 1 = \chi_\rho(\pi)$. Senza perdita di generalità, suppongo ora che π sia un primo complesso.

Se ρ è un primo complesso, vale che $p = \mathcal{N}(\pi)$ e $r = \mathcal{N}(\rho)$ sono primi razionali congrui a 1 modulo 3. Lavorando modulo ρ si ha:

$$g(\chi_\pi)^r = \left(\sum_{x\in\mathbb{F}_p} \chi_\pi(x)\zeta_p^x\right)^r \equiv \sum_{x\in\mathbb{F}_p} \chi_\pi^r(x)\zeta_p^{rx} = \chi_\pi^{-1}(r)\sum_{x\in\mathbb{F}_p} \chi_\pi(rx)\zeta_p^{rx} = \overline{\chi_\pi}(\rho\overline{\rho})g(\chi_\pi) \mod \rho,$$

dove si è usato che $\chi_\pi^r = \chi_\pi$ perché r è congruo a 1 modulo 3. Poiché $g(\chi_\pi)\overline{g(\chi_\pi)} = p \not\equiv 0 \mod \rho$, si ha che $g(\chi_\pi) \not\equiv 0 \mod \rho$: cancellandolo a destra e a sinistra dell'equazione si ha $g(\chi_\pi)^{r-1} \equiv \overline{\chi_\pi}(\rho\overline{\rho}) \mod \rho$. D'altronde, si ha:

$$g(\chi_\pi)^{r-1} = \left(g(\chi_\pi)^3\right)^{\frac{r-1}{3}} = (\pi^2\overline{\pi})^{\frac{r-1}{3}} \equiv \chi_\rho(\pi^2\overline{\pi}) \mod \rho.$$

Mettendo insieme le due espressioni si ottiene $\overline{\chi_\pi}(\rho\overline{\rho}) \equiv \chi_\rho(\pi^2\overline{\pi}) \mod \rho$, ma poiché ambo i lati dell'equazione sono unità, sono congrui modulo ρ se e solo se sono uguali come interi di Eisenstein, dunque $\overline{\chi_\pi}(\rho\overline{\rho}) = \chi_\rho(\pi^2\overline{\pi})$. Posso ripetere lo stesso procedimento scambiando π e ρ, ottenendo: $\overline{\chi_\rho}(\pi\overline{\pi}) = \chi_\pi(\rho^2\overline{\rho})$. In particolare, si ha $\chi_\pi(\rho\overline{\rho})\chi_\rho(\pi^2\overline{\pi}) = 1 = \chi_\rho(\pi\overline{\pi})\chi_\pi(\rho^2\overline{\rho})$. Cancellando i termini uguali da ambo i lati dell'equazione, si ottiene $\chi_\rho(\pi) = \chi_\pi(\rho)$.

Se $\rho = q \equiv 2 \mod 3$ è un primo razionale, $q^2 = \mathcal{N}(q)$ è congruo a 1 modulo 3. Lavorando modulo q si ha:

$$g(\chi_\pi)^{q^2} = \left(\sum_{x\in\mathbb{F}_p} \chi_\pi(x)\zeta_p^x\right)^{q^2} = \sum_{x\in\mathbb{F}_p} \chi_\pi^{q^2}(x)\zeta_p^{q^2x} = \chi_\pi(q)\sum_{x\in\mathbb{F}_p} \chi_\pi(q^2x)\zeta_p^{q^2x} = \chi_\pi(q)g(\chi_\pi) \mod q,$$

dove si è usato che $\chi_\pi^{q^2} = \chi_\pi$ perché q^2 è congruo a 1 modulo 3. Poiché $g(\chi_\pi)\overline{g(\chi_\pi)} = p \not\equiv 0 \mod q$, si ha che $g(\chi_\pi) \not\equiv 0 \mod q$: cancellandolo a destra e a sinistra dell'equazione si ha $g(\chi_\pi)^{q^2-1} \equiv \chi_\pi(q) \mod q$.

D'altronde, si ha:

$$g(\chi_\pi)^{q^2-1} = \left(g(\chi_\pi)^3\right)^{\frac{q^2-1}{3}} = (p\pi)^{\frac{q^2-1}{3}} \equiv p^{(q-1)\left(\frac{q+1}{3}\right)}\chi_q(\pi) \equiv \chi_q(\pi) \mod q.$$

Mettendo insieme le due espressioni si ottiene $\chi_\pi(q) \equiv \chi_q(\pi) \mod q$, ma poiché come nel caso precedente ambo i lati dell'equazione sono unità, $\chi_\pi(q) = \chi_q(\pi)$. □

Capitolo 5

Controesempi

Avendo presente un risultato come il teorema di Hasse-Minkowski è naturale chiedersi fino a che punto possa valere il principio locale-globale. Da un lato, lo stesso teorema di Hasse-Minkowski è valido anche sostituendo il campo base $\mathbb{Q}$ con un qualsiasi campo di numeri $\mathbb{K}$ e considerando i suoi completamenti rispetto ad ogni possibile norma moltiplicativa. D'altro canto, il principio locale-globale fallisce in casi analoghi in cui non si considerano equazioni quadratiche.

5.1 Controesempio di Lind-Reichardt

Proposizione 5.1.1 (Lind-Reichardt, [Rei42],[Lin40])**.** *L'equazione* $2y^2 = x^4 - 17z^4$ *ha uno zero non banale in ogni completamento* $\mathbb{Q}_v$*, ma non ne ammette nessuno in* $\mathbb{Q}$*.*

Dimostrazione. L'equazione ha chiaramente soluzione non banale su $\mathbb{R}$. Per quanto riguarda l'esistenza di soluzioni locali in $\mathbb{Q}_p$ con $p \neq 2$, basta dimostrare la tesi più forte che l'equazione $2y^2 - x^4 + 17 = 0$ ha uno zero non banale modulo p per ogni p primo, e tale che il gradiente della funzione, valutato in quel punto, sia diverso da 0. Ammesso che esista un tale zero non banale, il gradiente $(-4x^3, 4y)$ sarà diverso da 0, dunque per il lemma di Hensel-2 questo punto si solleverà ad uno zero non banale dell'equazione in $\mathbb{Q}_p$ per ogni $p \neq 2$. L'esistenza di soluzioni modulo p deriva dalle seguenti considerazioni.

Per $p = 17$ esiste la soluzione non banale $(6, 6)$. Se $p \neq 17$ ogni soluzione dell'equazione è non banale, dunque mi basta dimostrare che esista una soluzione.

Se $p \equiv 3 \mod 4$, si ha che ogni numero intero è un quadrato modulo p se e solo se è una potenza quarta modulo p. Dunque l'equazione considerata ha uno zero se e solo se ne ha l'equazione $2y^2 - z^2 + 17 = 0$. Se per assurdo questa non avesse soluzione, vorrebbe dire che $2y^2 + 17$ non è un quadrato modulo p per alcun valore di y. In altri termini, $\left(\frac{2y^2+17}{p}\right) = -1$ per ogni $y \in \mathbb{F}_p$, per cui lavorando modulo p si ottiene:

$$0 \equiv \sum_{y \in \mathbb{F}_p} \left(\frac{2y^2 + 17}{p}\right) \equiv \sum_{y \in \mathbb{F}_p} (2y^2 + 17)^{\frac{p-1}{2}} \mod p.$$

Se $a \geq 1$ non è multiplo di $p - 1$, si ha che $\sum_{y \in \mathbb{F}_p} y^a \equiv 0 \mod p$. Infatti, detto h un generatore

di $\mathbb{F}_p^*$, si ha che $h^a \neq 1$, dunque:

$$\sum_{x\in\mathbb{F}_p} x^a \equiv \sum_{n=0}^{p-2} h^{na} = \frac{1-h^{(p-1)a}}{1-h^a} = 0.$$

Poiché nel polinomio $(2y^2+17)^{\frac{p-1}{2}}$ l'unico termine di grado positivo multiplo di $p-1$ è il termine di testa, e poiché si sta sommando il termine noto p volte:

$$\sum_{y\in\mathbb{F}_p} (2y^2+17)^{\frac{p-1}{2}} \equiv \sum_{y\in\mathbb{F}_p} 2^{\frac{p-1}{2}} y^{p-1} \equiv \sum_{y\in\mathbb{F}_p^*} 2^{\frac{p-1}{2}} \equiv -\left(\frac{2}{p}\right) \not\equiv 0 \mod p.$$

Essendo giunti a un assurdo, devono esistere soluzioni all'equazione modulo p.

Se $p \equiv 1 \mod 4$, considero due caratteri di $\mathbb{F}_p^*$ di ordine 2 e 4, che chiamo rispettivamente χ_2 e χ_4 (in particolare, dato che esiste un unico carattere di ordine 2, $\chi_2 = \chi_4^2$, e consiste nel simbolo di Legendre). Voglio contare le coppie $(x,y) \in \mathbb{F}_p^2$ tali che $x^4 - 2y^2 = 17$. Fissati a e b, il numero di x tali che $x^4 = a$ è dato da $\sum_{i=0}^3 \chi_4^i(a)$ e il numero di y tali che $-2y^2 = b$ è dato da $\sum_{i=0}^1 \chi_2^i(-2b)$ (dove pongo $\chi_2^0 = \chi_4^0 = 1$ su ogni elemento di $\mathbb{F}_p$). Dunque il numero di soluzioni di $x^4 - 2y^2 = 17$ è dato da:

$$\sum_{a+b=17} \left(\sum_{i=0}^3 \chi_4^i(a)\right)\left(\sum_{i=0}^1 \chi_2^i(-2b)\right).$$

Scrivendo $a = 17c$ e $b = 17d$, la sommatoria diventa:

$$\begin{aligned}\sum_{c+d=1} \left(\sum_{i=0}^3 \chi_4^i(17c)\right)\left(\sum_{i=0}^1 \chi_4^{2i}(-34d)\right) &= \sum_{c+d=1}\sum_{i=0}^3\sum_{j=0}^1 \chi_4^i(17c)\chi_4^{2j}(-34d) \\ &= \sum_{i=0}^3\sum_{j=0}^1 \chi_4^i(17)\chi_4^{2j}(-34)J(\chi_4^i,\chi_4^{2j}).\end{aligned}$$

Se uno solo tra i e j vale 0, $J(\chi_4^i,\chi_4^{2j}) = 0$, mentre se entrambi sono 0 si ha $J(\chi_4^i,\chi_4^{2j}) = p$. Dunque il valore cercato diventa:

$$p + \chi_4(17)\chi_2(-34)J(\chi_4,\chi_2) + \chi_2(17)\chi_2(-34)J(\chi_2,\chi_2) + \overline{\chi_4}(17)\chi_2(-34)J(\overline{\chi_4},\chi_2).$$

Il secondo ed il quarto termine hanno norma $\sqrt{p}$. Per il terzo termine, si ha che:

$$\begin{aligned}|J(\chi_2,\chi_2)| &= \left|\sum_{x\in\mathbb{F}_p} \chi_2(x)\chi_2(1-x)\right| \\ &= \left|\sum_{x\in\mathbb{F}_p\setminus\{0,1\}} \chi_2(x)\chi_2(1-x)\right| \\ &\leq \sum_{x\in\mathbb{F}_p\setminus\{0,1\}} |\chi_2(x)\chi_2(1-x)| \\ &\leq p-2.\end{aligned}$$

Valutandolo modulo p si ha invece:

$$J(\chi_2,\chi_2) \equiv \sum_{x\in\mathbb{F}_p} x^{\frac{p-1}{2}}(1-x)^{\frac{p-1}{2}} \equiv \sum_{x\in\mathbb{F}_p} (-1)^{\frac{p-1}{2}} x^{p-1} \equiv -(-1)^{\frac{p-1}{2}}.$$

Poiché deve avere norma minore o uguale a $p-2$, si ha effettivamente l'uguaglianza $J(\chi_2,\chi_2) = -(-1)^{\frac{p-1}{2}}$. Sostituendo le uguaglianze e le disuguaglianze considerate si ottiene: $N > p-2\sqrt{p}-1$. In particolare, se $p \geq 7$, deve esistere almeno una soluzione. Per quanto riguarda il caso restante di $p = 5$, si verifica che $(x, y) = (0, 2)$ è una soluzione.

Resta da trovare una soluzione non banale in $\mathbb{Q}_2$. Considero $2y^2 - x^4 + 17$ come un polinomio in $\mathbb{Z}_2[x, y]$ e provo ad applicare il lemma di Hensel-3. Per farlo, mi serve un punto $(a, b) \in (\mathbb{Z}_2)^2$ tale che la norma 2-adica della funzione valutata nel punto sia minore del quadrato della norma 2-adica della sua derivata. In formule, serve che $\|2b^2 - a^4 + 17\|_2 < \|4b - 4a^3\|_2^2$, e basta prendere $(a, b) = (3, 0)$: il primo termine diventa $\|-64\|_2 = \frac{1}{64}$, mentre il secondo diventa $\|-108\|_2^2 = \frac{1}{16}$.

Per quanto riguarda la non esistenza di una soluzione globale, si può procedere per assurdo. Data una soluzione non banale (x, y, z), anche (qx, q^2y, qz) sarà soluzione per ogni $q \in \mathbb{Q}$. Detto d il minimo comune denominatore di x, y, z, $(x', y', z') := (dx, d^2y, dz)$ è una soluzione intera dell'equazione. Prendo ora $d' = \gcd(x', z')$, e considero $(a, b, c) := \left(\frac{x'}{d'}, \frac{y'}{d'^2}, \frac{z'}{d'}\right)$, che è anch'essa una soluzione dell'equazione, in cui a e c sono interi coprimi. Poiché $a, c \in \mathbb{Z}$, segue che $2b^2 \in \mathbb{Z}$, dunque che anche b è un numero intero. Considero un qualsiasi fattore primo p di b: ricordando che $2b^2 = a^4 - 17c^4$, $p \neq 17$, poiché altrimenti dovrei avere che $17|a^4$, dunque $17|a$, e quindi $17^2|a^4 - 2b^2 = 17c$, che a sua volta implica $17|c$, assurdo per coprimalità di a e c. Analogamente, $p \nmid c$, altrimenti si avrebbe $p \mid a$, violando ancora una volta la coprimalità. Modulo p ho che $a^4 \equiv_p 17c^4$, dunque $17 \equiv_p \left(\frac{a}{c}\right)^4$, e in particolare $\left(\frac{17}{p}\right) = 1$. Per reciprocità quadratica, se p è dispari si ha $\left(\frac{p}{17}\right) = 1$, e inoltre $\left(\frac{2}{17}\right) = 1$, quindi b è un quadrato modulo 17: $b \equiv_{17} d^2$. Valutando l'equazione di partenza modulo 17 si ha dunque $2d^4 \equiv_{17} a^4$. Poiché $17 \nmid d$ ottengo che $2 \equiv_{17} \left(\frac{a}{d}\right)^4$, che è assurdo perché 2 non è una potenza quarta modulo 17. □

5.2 Controesempio di Heath-Brown

In questa sezione si presenta un'altra interpretazione del principio locale-globale più restrittiva di quella presente nel teorema di Hasse-Minkowski e nel controesempio di Lind-Reichardt. In entrambi i casi ci si è chiesto se, dato un polinomio in più variabili, l'esistenza di soluzioni in ogni completamento di $\mathbb{Q}$ implicasse l'esistenza di soluzioni razionali. Un'altra domanda che è possibile porsi è se tale polinomio rispetti o meno l'*approssimazione debole*.

Definizione 5.2.1 (Approssimazione debole)**.** Sia $f \in \mathbb{Q}[x_1, \cdots, x_n]$ un polinomio a coefficienti razionali. Si dice che f rispetta l'approssimazione debole se, fissato un numero finito di posti P e preso per ogni $v \in P$ uno zero di f $(c_{v,1}, \cdots, c_{v,n}) \in \bigtimes_1^n \mathbb{Q}_v$ e un numero reale positivo δ_v, allora esiste sempre uno zero razionale di f, $(c_1, \cdots, c_n) \in \bigtimes_1^n \mathbb{Q}$, tale che per ogni $v \in P$ valga che $\|(c_1, \cdots, c_n) - (c_{v,1}, \cdots, c_{v,n})\|_v < \delta_v$.

Proposizione 5.2.2 (Heath-Brown, [Hea92])**.** *Data una quaterna di interi (x, y, z, w) tale che $x^3 + y^3 + z^3 - 2w^3 = 0$, uno tra x, y e z è multiplo di 6.*

Dimostrazione. Senza perdita di generalità dimostro la proposizione per una generica soluzione intera (x, y, z, w) con $\gcd(x, y, z, w) = 1$. Poiché non tutti tra x, y e z sono pari (altrimenti lo sarebbe anche w, contrariamente all'ipotesi di coprimalità), ma la somma dei loro cubi è pari, si

ha che 2 divide esattamente uno di loro tre. Similmente, studiando l'equazione modulo 9, si ha che esattamente uno tra x, y e z è multiplo di 3, senza perdita di generalità $3 \mid y$. Nell'anello a fattorizzazione unica $\mathbb{Z}(\omega)$, con $\omega = \frac{1+\sqrt{3}}{2}$, si ha $(x+y)(x+\omega y)(x+\bar{\omega} y) = 2w^3 - z^3$. Sia π un divisore primo di $x + \omega y$: è sicuramente diverso da 2 perché almeno uno tra x e y è dispari. Inoltre, poiché $3 \mid y$ e $3 \nmid x$, si ha che $3 \nmid x^3 + y^3$, dunque $\pi \nmid 3$. Poiché $\pi \mid x + \omega y$, vale $z^3 \equiv_\pi 2w^3$, dunque se w è invertibile modulo π si ha che $\left(\frac{2}{\pi}\right)_3 = 1$. Se invece $\pi \mid w$, si ha $\pi \mid z$, dunque $\pi \nmid \gcd(x, y)$ per coprimalità della soluzione. Da questo segue che $\pi \nmid x + y, x + \omega^2 y$, dunque, detto e l'esponente tale che $\pi^e \parallel x + \omega y$, si ha $\pi^e \parallel 2w^3 - z^3$. Se 2 non è un cubo modulo π, vale che $\pi^e \parallel \gcd(w^3, z^3)$, dunque $3 \mid e$. Ricapitolando, preso π divisore primo di $x + \omega y$, si ha o che $\left(\frac{2}{\pi}\right)_3 = 1$, e dunque per reciprocità cubica, essendo $\pi \nmid 3$, vale che $\left(\frac{\pi}{2}\right)_3 = 1$, o che $3 \mid e$, dove e è tale che $\pi^e \parallel x + \omega y$, dunque $\left(\frac{\pi^e}{2}\right)_3 = 1$. Per linearità, facendo il prodotto al variare dei divisori primi di $x + \omega y$, si ottiene $\left(\frac{x+\omega y}{2}\right)_3 = 1$. Pertanto, esistono $a, b \in \mathbb{Z}$ tali che $x + \omega y \equiv_2 (a + \omega b)^3 = (a^3 - 3ab^2 + b^3) + \omega(3a^2 b - 3ab^2)$, dunque $y \equiv_2 3ab(a - b) \equiv_2 0$. Insieme all'ipotesi iniziale, si ottiene che $6 \mid y$. □

Corollario 5.2.3. *La forma $x^3 + y^3 + z^3 - 2w^3$ non rispetta l'approssimazione debole.*

Dimostrazione. Considero i due zeri $(1, 1, 0, 1) \in \mathbb{Q}_2$ e $(1, 0, 1, 1) \in \mathbb{Q}_3$. Per assurdo, se la forma rispetta l'approssimazione debole, esiste uno zero razionale (x, y, z, w) arbitrariamente vicino a questi due in norma 2-adica e 3-adica rispettivamente. In particolare, esiste una soluzione razionale con $v_2(x) = v_2(y) = v_2(w) = 0$, $v_2(z) \geq 0$ e con $v_3(x) = v_3(z) = v_3(w) = 0$, $v_3(y) \geq 0$. Dunque il minimo comune denominatore d di x, y, z, w, scritti come frazioni ridotte ai minimi termini, non è divisibile né per 2 né per 3: la quaterna (dx, dy, dz, dw) è composta di numeri interi ed è uno zero della forma, inoltre valgono le stesse stime in termini di valutazioni 2-adiche e 3-adiche, per cui nessuno tra dx, dy, dz è multiplo di 6, il che è assurdo per la proposizione precedente. □

5.3 Controesempio di Selmer

Il controesempio forse più significativo di questa sezione è però dovuto a Selmer: esso offre un esempio di forma cubica che non rispetta il principio locale-globale nella sua accezione più ampia.

Proposizione 5.3.1 (Selmer, [Con])**.** *L'equazione $f(x, y, z) = 3x^3 + 4y^3 + 5z^3 = 0$ ammette soluzione non banale su tutti i $\mathbb{Q}_p$ ma non su $\mathbb{Q}$.*

Dimostrazione. In primo luogo, dimostro che l'equazione ammette sempre una soluzione locale non banale. Su $\mathbb{R}$ esistono ovviamente zeri non banali dell'equazione.

Se $p = 3$, considero il polinomio $g(y) = 4y^3 - 5$. Prendo l'elemento $\alpha = 2$ di $\mathbb{Z}_3$, e ho $\|g(\alpha)\|_3 = \|27\|_3 = \frac{1}{27}$, mentre valutando la derivata ho $\|g'(\alpha)\|_3 = \|48\|_3 = \frac{1}{3}$. Valgono le ipotesi del lemma di Hensel-3, dunque esiste una radice $\alpha^* \in \mathbb{Z}_3$ di g con $\|\alpha^* - \alpha\|_3 < \frac{1}{9}$. Di conseguenza, $(0, \alpha^*, -1)$ è uno zero non banale di f in $\mathbb{Q}_3$.

Per i primi restanti:

- se 3 è un cubo modulo p (ad esempio per $p = 2, 5$), posto $3 \equiv a^3 \not\equiv 0 \mod p$ si ha che $f\left(\frac{1}{a}, 1, -1\right) \equiv 0 \mod p$ e che $\frac{\partial f}{\partial x}\left(\frac{1}{a}, 1, -1\right) \equiv \frac{9}{a^2} \equiv 3a \not\equiv 0 \mod p$;
- se 2 è un cubo modulo p (e $p \neq 2$), posto $2 \equiv b^3 \not\equiv 0 \mod p$ si ha che $f\left(1, \frac{1}{b}, -1\right) \equiv 0 \mod p$ e che $\frac{\partial f}{\partial y}\left(1, \frac{1}{b}, -1\right) \equiv \frac{12}{b^2} \equiv 6b \not\equiv 0 \mod p$;
- se 5 è un cubo modulo p (e $p \neq 5$), posto $5 \equiv c^3 \not\equiv 0 \mod p$ si ha che $f\left(1, -1, \frac{1}{c}\right) \equiv 0 \mod p$ e che $\frac{\partial f}{\partial z}\left(1, -1, \frac{1}{c}\right) \equiv \frac{15}{c^2} \equiv 3c \not\equiv 0 \mod p$.

In tutti e tre i casi, per il lemma di Hensel-2 posso sollevare la soluzione (non banale) modulo p a una soluzione (non banale) in $\mathbb{Q}_p$.

Avendo affrontato i casi $p = 2, 3, 5$, rimangono solo i casi in cui p non divide alcun coefficiente o esponente di f e nessuno tra 3, 4 e 5 è un cubo modulo p. Considero i tre valori $3^{\frac{p-1}{3}}, 4^{\frac{p-1}{3}}, 5^{\frac{p-1}{3}}$ modulo p: questi sono radici cubiche dell'unità in $\mathbb{F}_p$, ma sono tutte diverse da 1 perché 3, 4 e 5 non sono cubi modulo p. Pertanto due di questi valori sono uguali, e almeno uno tra i loro rapporti $\frac{3}{4}^{\frac{p-1}{3}}, \frac{4}{5}^{\frac{p-1}{3}}, \frac{5}{3}^{\frac{p-1}{3}}$ è pari a 1, dunque almeno uno tra $\frac{3}{4}$, $\frac{4}{5}$ e $\frac{5}{3}$ è un cubo modulo p. Se ad esempio $\frac{3}{4}$ è il cubo, e pongo $\frac{3}{4} \equiv d^3 \mod p$, ho che $f(-1, d, 0) \equiv 0 \mod p$ e che $\frac{\partial f}{\partial x}(-1, d, 0) = 3 \not\equiv 0 \mod p$, dunque per il lemma di Hensel-2 $(-1, d, 0)$ si solleva a uno zero di f (non banale) in $\mathbb{Q}_p$. Si procede in maniera del tutto analoga se il cubo è $\frac{4}{5}$ o $\frac{5}{3}$.

Serve ora dimostrare la non esistenza di una soluzione globale.

Con il cambio di variabili $X = 2y, Y = x, Z = -z$ e moltiplicando per 2 ottengo la nuova equazione:

$$X^3 + 6Y^3 = 10Z^3.$$

Poiché l'equazione è omogenea, posso riscalare tutte le incognite per uno stesso numero razionale, dunque senza perdita di generalità assumo che X, Y, Z siano interi e che non esista alcun fattore primo che li divida tutti. Posso subito ottenere dei risultati di divisibilità.

- Poiché $2|10Z^3 - 6Y^3$, ho $2|X^3$, quindi $2|X$.
- Poiché $3|10Z^3 - X^3$, se 3 dividesse uno tra X e Z, dividerebbe anche l'altro e si avrebbe $3^3|10Z^3 - X^3$, quindi $3^3|6Y^3$ e $3|Y$; ma allora 3 sarebbe fattore comune a X, Y e Z, che è assurdo. Si ha quindi $3 \nmid X$, $3 \nmid Z$.
- Poiché $5|X^3 + 6Y^3$, se 5 dividesse uno tra X e Y, dividerebbe anche l'altro e si avrebbe $5^3|X^3 + 6Y^3$, quindi $5^3|10Z^3$ e $5|Z$; ma allora 5 sarebbe fattore comune a X, Y e Z, che è assurdo. Si ha quindi $5 \nmid X$, $5 \nmid Y$.

Studio ora l'equazione sull'anello $\mathbb{Z}[\alpha]$, dove $\alpha = \sqrt[3]{6}$. L'obiettivo di questa parte della dimostrazione è provare che $\mathbb{Z}[\alpha]$ coincide con l'anello degli interi del suo campo delle frazioni $\mathbb{Q}(\alpha)$: in tal caso, $\mathbb{Z}[\alpha]$ sarebbe un dominio di Dedekind, dunque esisterebbe la fattorizzazione unica degli ideali.

Per prima cosa, occorre trovare il discriminante dell'anello $\mathbb{Z}[\alpha]$. In generale, dato $d \in \mathbb{Z}$ non cubo, gli omomorfismi di campi da $\mathbb{Q}(\sqrt[3]{d})$ a $\mathbb{C}$ sono solo 3, ossia $\sigma_i(\sqrt[3]{d}) = \zeta_3^i \sqrt[3]{d}$ per $i = 0, 1, 2$, pertanto dalla definizione di discriminante si ha che $disc(\mathbb{Z}[\sqrt[3]{d}])$ è pari a:

$$disc(1, \sqrt[3]{d}, \sqrt[3]{d^2}) = \det \begin{pmatrix} \sigma_0(1) & \sigma_0(\sqrt[3]{d}) & \sigma_0(\sqrt[3]{d^2}) \\ \sigma_1(1) & \sigma_1(\sqrt[3]{d}) & \sigma_1(\sqrt[3]{d^2}) \\ \sigma_1(1) & \sigma_2(\sqrt[3]{d}) & \sigma_2(\sqrt[3]{d^2}) \end{pmatrix}^2 = \begin{pmatrix} 1 & \sqrt[3]{d} & \sqrt[3]{d^2} \\ 1 & \zeta_3 \sqrt[3]{d} & \zeta_3^2 \sqrt[3]{d^2} \\ 1 & \zeta_3^2 \sqrt[3]{d} & \zeta_3 \sqrt[3]{d^2} \end{pmatrix}^2 = -27d^2.$$

Inoltre, posti $A = \mathbb{Z}[\sqrt[3]{d}]$ e $\mathcal{O}$ l'anello degli interi di $\mathbb{Q}(\sqrt[3]{d})$, si ha $disc(A) = [\mathcal{O} : A]^2 disc(\mathcal{O})$. Poiché $disc(A) = 27d^2$, si ha che $[\mathcal{O} : A]$, detto anche *indice* di $\sqrt[3]{d}$, divide $3d$. Nel caso in analisi, poiché $d = 6$, l'indice di α divide 18. Tuttavia il polinomio minimo di α su $\mathbb{Z}$, ossia $\mu_\alpha(T) = T^3 - 6$, è p-Eisentein per $p = 2, 3$, dunque l'indice di α non può essere multiplo di 2 o di 3, ed è pertanto pari a 1: in altre parole, l'anello degli interi di $\mathbb{Q}(\alpha)$ è proprio $\mathbb{Z}[\alpha]$, e in particolare $\mathbb{Z}[\alpha]$ è un dominio di Dedekind.

Ricordo che esiste una norma moltiplicativa sugli ideali I di $\mathbb{Z}[\alpha]$, definita come $\mathcal{N}(I) = |\mathbb{Z}[\alpha]/I|$; inoltre, se l'ideale è principale e $I = (x + \alpha y)$, vale $\mathcal{N}(I) = \|x^3 + 6y^3\|$. Infine, gli ideali primi di $\mathbb{Z}[\alpha]$ hanno tutti come norma una potenza di p, dove p è un numero primo di $\mathbb{Z}$, e sono tutti e soli gli ideali che compaiono nella fattorizzazione di (p).

Per il teorema di Kummer, dato che $\mathbb{Z}[\alpha]$ coincide con l'anello degli interi di $\mathbb{Q}(\alpha)$, per ogni primo p di $\mathbb{Z}$ la fattorizzazione dell'ideale (p) in $\mathbb{Z}[\alpha]$ "rispecchia" la fattorizzazione di μ_α su $\mathbb{F}_p$. Per la precisione, se $\mu_\alpha = f_1^{a_1} \cdots f_n^{a_n}$ è la fattorizzazione di μ_α in polinomi irriducibili modulo p, dove f_i ha grado d_i, allora $(p) = P_1^{a_1} \cdots P_n^{a_n}$, dove i P_i sono ideali primi distinti, P_i divide l'ideale $(f_i(\alpha))$ (che non è l'ideale (0) se la fattorizzazione non è banale) e $\mathcal{N}(I_i) = p^{a_i}$.

In particolare, poiché $\mu_\alpha(T) \equiv T^3$ modulo 2 e modulo 3, $\mu_\alpha(T) \equiv (T-1)(T^2+T+1) \mod 5$, e $\mu_\alpha(T) \equiv (T+1)(T+2)(T+4) \mod 7$, si ha $(2) = \mathfrak{p}_2^3$, $(3) = \mathfrak{p}_3^3$, $(5) = \mathfrak{p}_5\mathfrak{p}_{25}$ e $(7) = \mathfrak{p}_7\mathfrak{p}_7'\mathfrak{p}_7''$, dove $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_5, \mathfrak{p}_{25}, \mathfrak{p}_7, \mathfrak{p}_7', \mathfrak{p}_7''$ sono ideali primi di $\mathbb{Z}[\alpha]$ la cui norma è indicata al loro pedice. Inoltre, questi sono tutti e soli gli ideali primi di $\mathbb{Z}[\alpha]$ con norma divisibile per 2, 3, 5 o 7.

L'obiettivo è ora dimostrare che $\mathbb{Z}[\alpha]$ è un dominio a ideali principali, o equivalentemente dimostrare che il suo gruppo delle classi di ideali è banale. Grazie al teorema di Minkowski, ogni elemento del gruppo delle classi ha come rappresentante un ideale $I \subseteq \mathbb{Z}[\alpha]$ con $\mathcal{N}(I) < \lambda$, dove λ è dato dalla formula seguente:

$$\lambda = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|disc(\mathbb{Z}[\alpha])|},$$

con $n = [\mathbb{Q}(\alpha) : \mathbb{Q}] = r + 2s$, dove r indica il numero di omomorfismi reali da $\mathbb{Q}(\alpha)$ in $\mathbb{C}$ e s il numero di omomorfismi complessi a meno di coniugio. Nel caso in esame, $n = 3$, $s = 1$ e $disc(\mathbb{Z}[\alpha]) = -27 \cdot 6^2$, dunque:

$$\lambda = \frac{6}{27} \left(\frac{4}{\pi}\right) \sqrt{27 \cdot 6^2} = \frac{16\sqrt{3}}{\pi} \approx 8.82.$$

Se ogni ideale primo di norma minore di λ appartiene alla classe banale, ossia è generato da un solo elemento, allora il gruppo delle classi è banale: poiché gli ideali primi hanno come norma la potenza di un numero primo, devo controllare gli ideali di norma $2, 3, 4, 5, 7, 8$. Tuttavia, come dimostrato precedentemente, gli unici ideali di norma 2, 3 e 5 sono rispettivamente $\mathfrak{p}_2$, $\mathfrak{p}_3$ e $\mathfrak{p}_5$, gli unici ideali di norma 7 sono $\mathfrak{p}_7$, $\mathfrak{p}_7'$ e $\mathfrak{p}_7''$, e non esistono ideali primi di norma 4 o 8 (poiché non compaiono nella fattorizzazione di (2)). Per quanto riguarda i primi tre ideali, noto che:

$$\begin{aligned}
&\mathcal{N}((\alpha-2)) = |(-2)^3 + 6 \cdot 1^2| = 2 \Longrightarrow (\alpha-2) = \mathfrak{p}_2;\\
&\mathcal{N}((\alpha-1)) = |(-1)^3 + 6 \cdot 1^2| = 5 \Longrightarrow (\alpha-1) = \mathfrak{p}_5;\\
&\mathcal{N}((\alpha)) = 6 \Longrightarrow (\alpha) = \mathfrak{p}_2\mathfrak{p}_3.
\end{aligned}$$

Da quest'ultima considerazione, poiché il prodotto di $\mathfrak{p}_3$ con un ideale principale restituisce un ideale principale, anche $\mathfrak{p}_3$ deve essere un ideale principale. Infine, dalla fattorizzazione modulo 7 del polinomio minimo di α si ha che $\mathfrak{p}_7|(\alpha+1)$, $\mathfrak{p}_7'|(\alpha+2)$ e $\mathfrak{p}_7''|(\alpha+4)$. Ragionando nuovamente con le norme e sfruttando che gli unici ideali di norma 2 e 5 sono $\mathfrak{p}_2$ e $\mathfrak{p}_5$ rispettivamente, si ha:

$$\begin{aligned}
&\mathcal{N}((\alpha+1)) = |1^3 + 6 \cdot 1^2| = 7 \Longrightarrow (\alpha+1) = \mathfrak{p}_7;\\
&\mathcal{N}((\alpha+2)) = |2^3 + 6 \cdot 1^2| = 14 \Longrightarrow (\alpha+2) = \mathfrak{p}_2\mathfrak{p}_7';\\
&\mathcal{N}((\alpha+4)) = |4^3 + 6 \cdot 1^2| = 70 \Longrightarrow (\alpha+4) = \mathfrak{p}_2\mathfrak{p}_5\mathfrak{p}_7''.
\end{aligned}$$

Analogamente a prima, si deduce che $\mathfrak{p}_7$, $\mathfrak{p}_7'$ e $\mathfrak{p}_7''$ sono tutti ideali principali. Di conseguenza, l'anello $\mathbb{Z}[\alpha]$ è effettivamente un dominio a ideali principali, e in particolare è un dominio a fattorizzazione unica. Di seguito si utilizzerà la fattorizzazione di ideali: in tal modo, non ci si

dovrà preoccupare della presenza di unità. Fattorizzo l'equazione di partenza, ottenendo:

$$(X+\alpha Y)(X^2-\alpha XY+\alpha^2Y^2)=\mathfrak{p}_2^3\mathfrak{p}_5\mathfrak{p}_{25}(Z)^3.$$

Voglio trovare il massimo comun divisore dei due ideali a sinistra, che chiamo (d). Poiché d divide sia $X+\alpha Y$ che $X^2-\alpha XY+\alpha^2Y^2$, divide anche $(X+\alpha Y)^3-(X^2-\alpha XY+\alpha^2Y^2)=3\alpha XY$. Sia $\mathfrak{p}=(p)$ un ideale primo che divide (d).

- Se $p\nmid 3\alpha$, p deve dividere uno tra X e Y, ma poiché divide anche $X+\alpha Y$ e non divide α, p divide sia X che Y. Ma poiché $\mathfrak{p}\neq\mathfrak{p}_2$ e $\mathfrak{p}^2|$LHS, si ha $\mathfrak{p}^2|$RHS, dunque $\mathfrak{p}|(Z)$, che è assurdo perché X, Y e Z sono coprimi.

- Se $p|3\alpha$, $\mathfrak{p}$ può essere solo $\mathfrak{p}_2$ o $\mathfrak{p}_3$. Tuttavia, come osservato inizialmente, $3\nmid Z$, che è un numero intero, dunque a maggior ragione $\mathfrak{p}_3\nmid$RHS, dunque non divide nemmeno il LHS.

Da queste considerazioni si ha che (d) è una potenza dell'ideale primo $\mathfrak{p}_2$. Inoltre, poiché 2 divide X ma non Y, $\mathfrak{p}_2^3|(X)$, ma $p_2||(\alpha Y)$, dunque $\mathfrak{p}_2||(X+\alpha Y)$; in particolare, $(d)|\mathfrak{p}_2$. D'altro canto, $\mathfrak{p}_2|(X^2-\alpha XY+\alpha^2Y^2)$, dunque $\mathfrak{p}_2|(d)$; pertanto, $(d)=\mathfrak{p}_2$. Poiché però $\mathfrak{p}_2^3||$RHS, deve dividere esattamente anche il LHS, e dato che $\mathfrak{p}_2||(X+\alpha Y)$, $\mathfrak{p}_2^2||(X^2-\alpha XY+\alpha^2Y^2)$.

Tornando all'equazione di partenza e guardandola modulo 5, si ottiene: $0\equiv_5 X^3+6Y^3\equiv_5 X^3+Y^3\equiv_5(X+Y)(X^2-XY+Y^2)$. Poiché il secondo fattore è sempre diverso da 0 modulo 5, si ha che $5|X+Y$. In particolare, poiché $\mathfrak{p}_5=(\alpha-1)$, e dunque $\alpha-1|5$, si ha che $\alpha-1|X+Y-(\alpha-1)Y=X+\alpha Y$. Se anche $\mathfrak{p}_{25}$ dividesse $(X+\alpha Y)$ si avrebbe che $5|X+\alpha Y$, dunque dovrebbe dividere sia X che Y, che è assurdo per quanto osservato inizialmente. Poiché però $\mathfrak{p}_{25}$ divide il RHS, deve dividere anche il LHS, e dunque $\mathfrak{p}_{25}|(X^2-\alpha XY+\alpha^2Y^2)$.

Da questi ragionamenti otteniamo che $(X+\alpha Y)=\mathfrak{p}_2\mathfrak{p}_5I$ e $(X^2-\alpha XY+\alpha^2Y^2)=\mathfrak{p}_2^2\mathfrak{p}_{25}J$, dove I e J sono opportuni ideali di $\mathbb{Z}[\alpha]$; inoltre, I e J non hanno fattori comuni. Sostituendo nell'equazione si ha:

$$\mathfrak{p}_2\mathfrak{p}_5I\cdot\mathfrak{p}_2^2\mathfrak{p}_{25}J=\mathfrak{p}_2^3\mathfrak{p}_5\mathfrak{p}_{25}(Z)^3;$$
$$IJ=(Z)^3.$$

Essendo I e J coprimi, devono entrambi essere cubi di ideali: $I=(\beta)^3$ e $J=(\gamma)^3$, con $\beta,\gamma\in\mathbb{Z}[\alpha]$ coprimi.

A questo punto, si può tornare a ragionare in termini di elementi e scrivere:

$$X+\alpha Y=u(\alpha-2)(\alpha-1)\beta^3,$$

dove u è un'unità di $\mathbb{Z}[\alpha]$. Poiché ogni cubo nell'equazione può essere assorbito nel termine β^3, è sufficiente determinare la struttura delle unità di $\mathbb{Z}[\alpha]$ a meno di cubi. Il gruppo delle unità U è isomorfo a $\mathbb{Z}^n\oplus T$, dove n è un numero naturale e T è il sottogruppo di torsione dato dagli elementi di U che sono radici complesse dell'unità. Nel caso specifico, poiché $\mathbb{Z}[\alpha]\subseteq\mathbb{R}$, $T=\{\pm1\}$; inoltre, per il teorema delle unità di Dirichlet, $n=r+s-1$, dove r è il numero di embedding reali e s è il numero di embedding complessi a meno di coniugio del campo $\mathbb{Q}(\alpha)$, dunque $n=1$. Presa u un'unità che non sia un cubo in $\mathbb{Z}[\alpha]$, le unità a meno di cubi sono rappresentate dagli elementi $1,u,u^2$. Per trovare un'unità non banale di $\mathbb{Z}[\alpha]$ si può utilizzare il fatto che $(2)=\mathfrak{p}_2^3=(\alpha-2)^3=(2-\alpha)^3$, da cui si ricava l'unità $u=\frac{(2-\alpha)^3}{2}$. Per verificare che quest'unità non è un cubo, basta dimostrare che 2 non è un cubo. Se lo fosse, lo sarebbe anche modulo $\mathfrak{p}_7$, quindi per il piccolo teorema di Fermat si avrebbe $2^{\frac{\mathcal{N}(\mathfrak{p}_7)-1}{3}}\equiv 1 \mod \mathfrak{p}_7$. Dunque dovrebbe valere $0\equiv 2^{\frac{\mathcal{N}(\mathfrak{p}_7)-1}{3}}-1\equiv 2^2-1\equiv 3 \mod \mathfrak{p}_7$ e pertanto $\mathfrak{p}_7|(3)$, che è assurdo. Poiché

u non è un cubo, per qualche i che può valere 0, 1 o 2, si può scrivere:

$$\begin{aligned} X + \alpha Y &= u^i(\alpha - 2)(\alpha - 1)\beta^3; \\ X + \alpha Y &= \frac{(2-\alpha)^{3\,i}}{2}(\alpha - 2)(\alpha - 1)\beta^3; \\ 2^i X + \alpha 2^i Y &= (\alpha - 2)(\alpha - 1)\delta^3, \end{aligned}$$

dove $\delta = (2-\alpha)\beta$. Scrivendo $\delta = A + B\alpha + C\alpha^2$, dove $A, B, C \in \mathbb{Z}$, si può espandere il prodotto al RHS, sostituendo $\alpha^3 = 6$ e considerare l'equazione come un sistema di equazioni tra i coefficienti di 1, α e α^2. Considerando in particolare il termine in α^2, si ottiene:

$$A^3 + 6B^3 + 36C^3 + 36ABC - 9(A^2B + 6B^2C + 6C^2A) + 6(AB^2 + 6BC^2 + CA^2) = 0.$$

Poiché $\delta \neq 0$, questa equazione, pensata nelle variabili intere A, B e C, deve avere soluzioni non banali. Se ne ha, posso prendere una tale soluzione (A', B', C') in modo che A', B' e C' non abbiano un fattore comune: se ci fosse, potrei dividere per tale fattore, dato che l'equazione è omogenea, ottenendo la soluzione desiderata.

Poiché 3 divide tutti i monomi diversi da A'^3, deve valere $3|A'$. Ma allora 9 divide tutti i monomi diversi da $6B'^3$, dunque deve valere $3|B'$. Infine, si ha quindi che 27 divide tutti i monomi diversi da $36C'^3$, perciò deve valere $3|C'$. Ma allora 3 è un fattore comune di A', B' e C', contravvenendo all'ipotesi di coprimalità. Ne consegue che non esistono soluzioni intere non banali di quell'equazione, e pertanto non esiste il γ cercato, dunque non esistono soluzioni intere non banali all'equazione $X^3 + 6Y^3 = 10Z^3$.

□

Capitolo 6

Un approccio più generale

La dimostrazione del teorema di Hasse-Minkowski presentata nel capitolo 3 fa esplicito uso del fatto che $\mathbb{Q}$ sia il campo su cui è definita la forma quadratica. Il teorema è vero per qualsiasi campo di numeri $\mathbb{K}$, ma per arrivare a una dimostrazione è necessario un punto di vista completamente diverso sul problema. Per approfondimenti sugli strumenti utilizzati in questo capitolo, si rimanda a [Voi18].

6.1 Gruppo di Brauer e teorema di Brauer-Hasse-Noether

Per iniziare, è necessario presentare un oggetto cardine di questo capitolo, ossia il *gruppo di Brauer* di un campo $\mathbb{K}$. La struttura di questo gruppo verrà presentata in modo assiomatico, poiché la sua costruzione rigorosa esula dagli obiettivi di questa tesi.

Definizione 6.1.1. Un'*algebra centrale semplice* su un campo $\mathbb{K}$ è una $\mathbb{K}$-algebra priva di ideali bilateri propri e tale che il centro dell'algebra sia isomorfo a $\mathbb{K}$.

Un'*algebra di divisione* su un campo $\mathbb{K}$ è una $\mathbb{K}$-algebra tale che tutti i suoi elementi x diversi da 0 abbiano un inverso bilatero x^{-1}, ossia tale che $x \cdot x^{-1} = 1 = x^{-1} \cdot x$.

Teorema 6.1.2 (Wedderburn, [Voi18, Teorema 7.3.10])**.** *Sia A un'algebra centrale semplice di dimensione finita su un campo $\mathbb{K}$. Allora esiste un unico numero naturale n e un'unica algebra di divisione su K (a meno di isomorfismo) D, tali che A sia isomorfa come $\mathbb{K}$-algebra all'algebra di matrici $M_n(D)$.*

Definizione 6.1.3 (Gruppo di Brauer, [Mil13, cap.4])**.** Si consideri l'insieme X delle algebre centrali semplici di dimensione finita su $\mathbb{K}$: risulta chiuso rispetto al prodotto tensore, dunque ha una struttura di monoide. Sia $\mathcal{R}$ la seguente relazione di equivalenza su X: dati due elementi $A, A' \in X$, se $A \cong M_n(D)$ e $A' \cong M_{n'}(D')$, dove D e D' sono algebre di divisione su $\mathbb{K}$, $A\mathcal{R}A'$ se e solo se D e D' sono isomorfe come $\mathbb{K}$-algebre. Preso l'insieme $X/\mathcal{R}$, l'operazione binaria $[\otimes] : ([A], [B]) \mapsto [A \otimes B]$ è ben definita e conferisce all'insieme una struttura di gruppo. Si pone dunque $Br(\mathbb{K}) := X/\mathcal{R}$, e viene detto *gruppo di Brauer* di $\mathbb{K}$.

Il gruppo di Brauer ha un ruolo nella dimostrazione del teorema di Hasse-Minkowski nella sua forma più generale mediante il seguente risultato (di cui ancora una volta non si riporta la dimostrazione).

Teorema 6.1.4 (Brauer-Hasse-Noether, [Mil13, Teorema 4.2])**.** *Sia $\mathbb{K}$ un campo di numeri. Indicando con v i suoi posti, si ha la seguente successione esatta corta di gruppi abeliani:*

$$0 \longrightarrow Br(\mathbb{K}) \xrightarrow{i} \bigoplus_v Br(\mathbb{K}_v) \xrightarrow{inv} \mathbb{Q}/\mathbb{Z} \longrightarrow 0,$$

dove le mappe sono così definite:

- *i è la mappa che manda la classe di equivalenza $[E]$ di una $\mathbb{K}$-algebra E in $([E_v])_v \in \prod_v Br(\mathbb{K}_v)$, dove $[E_v]$ è la classe di equivalenza in $Br(\mathbb{K}_v)$ dell'algebra $E_v := E \otimes \mathbb{K}_v$.*
- *inv è la somma degli invarianti locali $inv_v : Br(\mathbb{K}_v) \to \mathbb{Q}/\mathbb{Z}$.*

Osservazione 6.1.5. A priori, la mappa i ha immagine in $\prod_v Br(\mathbb{K}_v)$. Il fatto che l'immagine sia contenuta in $\bigoplus_v Br(\mathbb{K}_v)$ è un risultato di per sé non immediato: come si vedrà nella prossima sezione, nel caso particolare in cui $\mathbb{K} = \mathbb{Q}$, e considerando i soli elementi di 2-torsione, corrisponde al fatto che per ogni coppia di razionali a e b il simbolo di Hilbert $(a, b)_v$ è diverso da 1 per un numero finito di posti v.

La definizione della mappa $inv_v : Br(\mathbb{K}_v) \to \mathbb{Q}/\mathbb{Z}$ non è necessaria per comprendere il collegamento tra il teorema di Brauer-Hasse-Noether e quello di Hasse-Minkowski: come si vedrà nella sezione 5.3, l'informazione essenziale ricavata da questo teorema è l'iniettività della mappa i.

6.2 Algebre di quaternioni

Lo scopo di questa sezione è evidenziare il legame tra le forme quadratiche ternarie a coefficienti in un campo generico $\mathbb{K}$ e le algebre di quaternioni su $\mathbb{K}$. Iniziamo appunto con la seguente definizione:

Definizione 6.2.1. Sia $\mathbb{K}$ un campo e siano $a, b \in \mathbb{K}^*$. Si consideri lo spazio vettoriale $H_{\mathbb{K}}(a, b) := \mathbb{K} \oplus i\mathbb{K} \oplus j\mathbb{K} \oplus k\mathbb{K}$, munito di un prodotto tale che le seguenti relazioni legano gli elementi i, j, k:

$$i^2 = a,\ j^2 = b,\ ij = -ji = k.$$

$H_{\mathbb{K}}(a, b)$ è detta un'*algebra di quaternioni* su $\mathbb{K}$.

Definizione 6.2.2. Sia $\mathbb{H}$ un'algebra di quaternioni sul campo $\mathbb{K}$.

L'*involuzione standard* su $\mathbb{H}$ è l'applicazione $\mathbb{K}$-lineare:

$$\bar{\cdot} : \mathbb{H} \to \mathbb{H}$$
$$w + xi + yj + zk \mapsto w - xi - yj - zk.$$

La *norma ridotta* è la mappa $nrd : \mathbb{H} \to \mathbb{K}$ che manda l'elemento u in $u\bar{u}$.

La *traccia ridotta* è la mappa $trd : \mathbb{H} \to \mathbb{K}$ che manda l'elemento u in $u + \bar{u}$.

Osservazione 6.2.3. Le mappe di cui sopra sono ben definite. Inoltre, la norma ridotta è moltiplicativa e la traccia ridotta è additiva e $\mathbb{K}$-lineare.

Le proposizioni che seguono hanno lo scopo di provare il seguente risultato:

Proposizione 6.2.4. *Le algebre centrali semplici di dimensione 4 su un campo $\mathbb{K}$ sono tutte e sole le algebre di quaternioni.*

Una conseguenza del teorema di Wedderburn è che le algebre centrali semplici di dimensione 4 su un campo $\mathbb{K}$ possono essere solo algebre di divisione o algebre di matrici. Per quanto riguarda le prime, vale la seguente proposizione.

Proposizione 6.2.5. *Ogni algebra di divisione $\mathbb{H}$ di dimensione 4 su $\mathbb{K}$ con centro $\mathbb{K}$ è un'algebra di quaternioni.*

Dimostrazione. Sia x un elemento di $\mathbb{H}\backslash\mathbb{K}$. $\mathbb{K}[x]$ è commutativo, dunque è un campo (e in particolare è diverso da $\mathbb{H}$); inoltre, vale la formula sui gradi delle estensioni:

$$4 = \big[\mathbb{H} : \mathbb{K}\big] = \big[\mathbb{H} : \mathbb{K}[x]\big]\big[\mathbb{K}[x] : \mathbb{K}\big],$$

e poiché $\mathbb{K} \subsetneq \mathbb{K}[x] \subsetneq \mathbb{H}$ deve valere $[\mathbb{K}[x] : \mathbb{K}] = 2$. Da questo si deduce che ogni elemento $x \in \mathbb{H}\backslash\mathbb{K}$ ha come polinomio minimo su $\mathbb{K}$ un certo polinomio μ_x, di grado 2. Prendo uno qualsiasi di questi x, con $\mu_x(t) = t^2 - 2ct + d$: detti $i := x - c \notin \mathbb{K}$ e $a := d - c^2$, si ha che:

$$i^2 = (x-c)^2 = x^2 - 2cx + c^2 = \mu_x(x) + c^2 - d = c^2 - d = -a.$$

$\mathbb{H}$ non è commutativo, dunque esiste un elemento $y \in \mathbb{H}\backslash\mathbb{K}$ tale che $iy \neq yi$. Considero l'applicazione $\mathbb{K}[i]$-lineare T che moltiplica a destra per i. Si ha che il suo polinomio minimo è $T^2 + a = 0$, dunque si può scrivere $\mathbb{H}$ come somma diretta di autospazi di dimensione 1 su $\mathbb{K}[i]$: quello relativo all'autovalore i è proprio $\mathbb{K}[i]$, mentre chiamo V quello relativo all'autovalore $-i$: ho che $xi = -ix$ per ogni $x \in V$, e anche $x^2 i = -xix = ix^2$, dunque $x^2 \in \mathbb{K}[i]$. Prendo il polinomio minimo di un qualsiasi elemento j di $V\backslash\{0\}$ su $\mathbb{K}$, ricordando che deve avere necessariamente grado 2, poiché $j \in \mathbb{H}\backslash\mathbb{K}$: $\mu_j(t) = t^2 + et + f$. Poiché $j^2 + f \in \mathbb{K}[i]$ e $j^2 + ej + f = 0$, si ha $ej \in \mathbb{K}[i]$, ma dato che $e \in \mathbb{K}$ e $j \in V$, si ha $ej \in \mathbb{K}[i] \cap V = \{0\}$, e poiché $j \neq 0$, deve valere $e = 0$. Pertanto pongo $b := f$, e poiché $ij = -ji, i^2 = -a, j^2 = -b$, si ha che $\mathbb{H} = \mathbb{H}_{\mathbb{K}}(a, b)$. □

Proposizione 6.2.6. *L'algebra di quaternioni $\mathbb{H}_{\mathbb{K}}(a, b)$ è centrale semplice.*

Dimostrazione. Dividiamo la dimostrazione in due casi:

- Se $a = c^2$ con $c \in \mathbb{K}$, considero il seguente isomorfismo di $\mathbb{K}$-spazi vettoriali $\phi : \mathbb{H}_{\mathbb{K}}(a, b) \to M_2(\mathbb{K})$:

$$\begin{aligned} 1 &\mapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}; \\ i &\mapsto \begin{bmatrix} c & 0 \\ 0 & -c \end{bmatrix}; \\ j &\mapsto \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix}; \\ k &\mapsto \begin{bmatrix} 0 & bc \\ -c & 0 \end{bmatrix}. \end{aligned}$$

  Questo isomorfismo è tale che $\phi(xy) = \phi(x)\phi(y)$ per ogni $x, y \in \mathbb{H}_{\mathbb{K}}(a, b)$, dunque è un isomorfismo di algebre. In particolare, poiché isomorfa ad un'algebra di matrici, $\mathbb{H}_{\mathbb{K}}(a, b)$ è semplice e ha centro $\mathbb{K}$.

- Se a non è un quadrato in $\mathbb{K}$, prendo $\mathbb{L} := \mathbb{K}[\sqrt{a}]$. Per quanto dimostrato sopra, $\mathbb{H}_{\mathbb{L}}(a, b) = \mathbb{H}_{\mathbb{K}}(a, b) \otimes_{\mathbb{K}} \mathbb{L}$ è isomorfa come algebra all'algebra di matrici $M_2(\mathbb{L})$, dunque è semplice. Se per assurdo $\mathbb{H}_{\mathbb{K}}(a, b)$ contenesse un ideale bilatero non banale I, questo in particolare sarebbe un $\mathbb{K}$-spazio vettoriale di dimensione compresa tra 1 e 3, dunque $I \otimes_{\mathbb{K}} \mathbb{L}$ sarebbe un $\mathbb{L}$-spazio vettoriale di dimensione compresa tra 1 e 3. Poiché I è un ideale bilatero di $\mathbb{H}_{\mathbb{K}}(a, b)$, $I \otimes_{\mathbb{K}} \mathbb{L}$ è un ideale bilatero di $\mathbb{H}_{\mathbb{L}}(a, b)$, ma ciò è assurdo perché per via della sua

dimensione è diverso da $\{0\}$ e da $\mathbb{H}_{\mathbb{L}}(a,b)$. Infine, per la centralità, basta osservare che il centro di un'algebra è uno spazio vettoriale, e che:

$$Z(\mathbb{H}_{\mathbb{L}}(a,b)) = Z(\mathbb{H}_{\mathbb{K}}(a,b) \otimes_{\mathbb{K}} \mathbb{L}) \supseteq Z(\mathbb{H}_{\mathbb{K}}(a,b)) \otimes_{\mathbb{K}} \mathbb{L}.$$

Dall'inclusione si ricava che la dimensione del centro di $\mathbb{H}_{\mathbb{L}}(a,b)$ come $\mathbb{L}$-spazio vettoriale è maggiore o uguale alla dimensione del centro di $\mathbb{H}_{\mathbb{K}}(a,b)$ come $\mathbb{K}$-spazio vettoriale, ma poiché $\mathbb{H}_{\mathbb{L}}(a,b)$ è un'algebra di matrici, il suo centro ha dimensione 1, pertanto anche il centro di $\mathbb{H}_{\mathbb{K}}(a,b)$ ha dimensione 1 e, poiché contiene $\mathbb{K}$, deve essere proprio $\mathbb{K}$.

□

Corollario 6.2.7. *L'isomorfismo costruito nella prima parte della dimostrazione ha come conseguenza che l'algebra di matrici $M_2(\mathbb{K})$ può essere pensata come una particolare algebra di quaternioni, ad esempio $\mathbb{H}_{\mathbb{K}}(1,1)$.*

Una volta trovata questa corrispondenza tra le algebre di quaternioni e le algebre semplici di dimensione 4, il seguente risultato collega l'algebra di quaternioni $\mathbb{H}_{\mathbb{K}}(a,b)$ al simbolo di Hilbert (a,b).

Teorema 6.2.8 (Teorema principale)**.** *Le seguenti proposizioni sono equivalenti:*

1. $\langle 1, -a, -b, ab\rangle_{\mathbb{K}}$ *è isotropa;*
2. $\langle -a, -b, ab\rangle_{\mathbb{K}}$ *è isotropa;*
3. $\mathbb{H}_{\mathbb{K}}(a,b) \cong M_2(\mathbb{K})$*;*
4. $(a,b)_{\mathbb{K}} = 1$.

Dimostrazione.

$\boxed{2 \Rightarrow 1}$ Se (x,y,z) è un vettore isotropo non banale per la seconda forma, $(0,x,y,z)$ lo è per la prima.

$\boxed{1 \Rightarrow 2}$ Il problema equivale a chiedersi se, sapendo che esiste $x \in \mathbb{H}_{\mathbb{K}}(a,b)$ tale che $nrd(x) = 0$, allora esiste anche $y \in \mathbb{H}_{\mathbb{K}}(a,b)$ tale che $trd(y) = nrd(y) = 0$. Se $trd(x) = 0$ non c'è nulla da dimostrare. Altrimenti, si può prendere $z \neq 0$ che sia ortogonale a x e a 1 rispetto al prodotto scalare $(\cdot,\cdot)$ indotto dalla forma. Poiché $trd(x_1x_2) = (x_1, x_2)$ per ogni $x_1, x_2 \in \mathbb{H}_{\mathbb{K}}(a,b)$, si ha che $trd(xz) = (x,z) = 0$ e $trd(z) = (1,z) = 0$. Da quest'ultima uguaglianza si ricava che $\bar{z} = -z$, dunque $trd(\bar{x}z) = (\bar{x},z) = (x,\bar{z}) = -(x,z) = 0$. Si ha che $xz + \bar{x}z = trd(x)z \neq 0$, dunque almeno uno tra xz e $\bar{x}z$ è diverso da 0 (senza perdita di generalità xz). Entrambi hanno traccia 0 e, per moltiplicatività della norma, vale che $nrd(xz) = nrd(\bar{x}z) = 0$, dunque $y = xz$ è proprio l'elemento cercato.

$\boxed{2 \Leftrightarrow 4}$ $(a,b)_{\mathbb{K}} = 1$ se e solo se la forma $\langle a, b, -1\rangle_{\mathbb{K}}$ è isotropa. Questa forma è equivalente alla forma $\langle -a^2b, -ab^2, ab\rangle_{\mathbb{K}} = -a^2bx^2 - ab^2y^2 + abz^2$, in cui ho moltiplicato tutti i coefficienti per $-ab$, che è a sua volta equivalente alla forma $\langle -b, -a, ab\rangle_{\mathbb{K}} = -bx'^2 - ay'^2 + abz^2$, in cui ho operato il cambio di variabile invertibile $x' = ax, y' = by$.

$\boxed{3 \Leftrightarrow 1}$ Se $\mathbb{H}_{\mathbb{K}}(a,b) \cong M_2(\mathbb{K})$ esiste un elemento $u = w + xi + yj + zk$ non invertibile. Allora $ndr(u) = u\bar{u}$ non è invertibile, ma è un elemento di $\mathbb{K}$, dunque è 0. Pertanto la forma $\langle 1, -a, -b, ab\rangle$ è isotropa.

Se $\mathbb{H}_{\mathbb{K}}(a,b) \ncong M_2(\mathbb{K})$, per il teorema di Wedderburn è un'algebra di divisione. Pertanto, ogni elemento $u = w+xi+yj+zk \neq 0$ è invertibile, dunque $ndr(u) \neq 0$, e $w^2 - ax^2 - by^2 + abz^2 \neq 0$. Per arbitrarietà nella scelta dei coefficienti di u, si ha che la forma $\langle 1, -a, -b, ab\rangle$ è non isotropa.

□

Proposizione 6.2.9. *Sia $\mathbb{K}$ un campo, $\mathbb{H} := \mathbb{H}_{\mathbb{K}}(a,b)$ una sua algebra di quaternioni e sia $\mathbb{L} := \mathbb{K}(\sqrt{d})$ una sua generica estensione di grado 2. Allora esiste un'immersione di $\mathbb{K}$ algebre $i : \mathbb{L} \hookrightarrow \mathbb{H}$ se e solo se $\mathbb{L} \otimes \mathbb{H} \cong M_2(\mathbb{L})$.*

Dimostrazione.

$\boxed{\Rightarrow}$ Sia $\mu := i(\sqrt{d})$, per cui $\mu^2 = i(\sqrt{d})^2 = i(\sqrt{d}^2) = i(d)$. In $\mathbb{L} \otimes_{\mathbb{K}} \mathbb{H}$ si ha:

$$(\sqrt{d} \otimes 1 + 1 \otimes \mu)(\sqrt{d} \otimes 1 - 1 \otimes \mu) = (\sqrt{d} \otimes 1)^2 - (1 \otimes \mu)^2 = d \otimes 1 - 1 \otimes d = 0.$$

Gli elementi $\sqrt{d} \otimes 1 + 1 \otimes \mu$ e $\sqrt{d} \otimes 1 - 1 \otimes \mu$ sono non nulli, poiché $\sqrt{d} \otimes 1$ e $1 \otimes \mu$ sono linearmente indipendenti. $\mathbb{L} \otimes_{\mathbb{K}} \mathbb{H}$ non può essere un'algebra di divisione, dunque è isomorfa ad un'algebra di matrici. Poiché ha dimensione 4 su $\mathbb{L}$, deve valere necessariamente $\mathbb{L} \otimes_{\mathbb{K}} \mathbb{H} \cong M_2(\mathbb{L})$.

$\boxed{\Leftarrow}$ Si possono distinguere due casi:

- Se $\mathbb{H} \cong M_2(\mathbb{K})$, si può prendere come i il seguente omomorfismo iniettivo di $\mathbb{K}$-spazi vettoriali:

$$1 \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix};$$
$$\sqrt{d} \mapsto \begin{bmatrix} 0 & d \\ 1 & 0 \end{bmatrix}.$$

  Questo omomorfismo commuta con il prodotto, dunque è un'immersione di $\mathbb{K}$-algebre.

- Se $\mathbb{H}$ è un'algebra di divisione, si ha che $\mathbb{L} \otimes_{\mathbb{K}} \mathbb{H} \cong M_2(\mathbb{L})$ se e solo se la forma $\langle -a, -b, ab\rangle$ è isotropa su $\mathbb{L}$, ossia se esistono $x, y, z, u, v, w \in \mathbb{K}$, non tutti nulli, tali che:

$$-a(x + u\sqrt{d})^2 - b(y + v\sqrt{d})^2 + ab(z + w\sqrt{d})^2 = 0.$$

  Separando i termini che moltiplicano $\sqrt{d}$ si ha:

$$\begin{cases} -ax^2 - by^2 + abz^2 + d(-au^2 - bv^2 + abw^2) = 0 \\ -axu - byv + abzw = 0 \end{cases}.$$

  Le due equazioni possono essere interpretate nel seguente modo, definendo $(\cdot,\cdot)$ il prodotto scalare indotto su $\mathbb{H}$ dalla forma $\langle -a, -b, ab\rangle$, e chiamando $\alpha := xi + yj + zk$ e $\beta := ui + vj + wk$:

$$\begin{cases} nrd(\alpha) + d \cdot nrd(\beta) = 0 \\ (\alpha, \beta) = 0 \end{cases}.$$

  Poiché α è ortogonale a β si ha $trd(\alpha\beta) = 0$. Poiché $\mathbb{H}$ è un'algebra di divisione e almeno uno tra α e β è diverso da 0, almeno uno avrà norma non nulla, e dunque,

dalla prima equazione, nessuno dei due avrà norma nulla. In particolare, si può definire $\gamma := \alpha\beta^{-1} \in \mathbb{H}$. Per questo elemento vale:

$$nrd(\gamma) = nrd(\alpha\beta^{-1}) = nrd(\alpha)nrd(\beta)^{-1} = -d;$$
$$trd(\gamma) = trd(\alpha\beta^{-1}) = (\alpha, \beta^{-1}) = (\alpha, \overline{\beta})nrd(\beta)^{-1} = -(\alpha, \beta)nrd(\beta)^{-1} = 0.$$

Da ciò si ricava che $d = -nrd(\gamma) = -\gamma\overline{\gamma} = \gamma^2$, dunque si può prendere come i l'omomorfismo iniettivo di $\mathbb{K}$-spazi vettoriali che manda k in $k \otimes 1$ per ogni $k \in \mathbb{K}$ e manda $\sqrt{d}$ in γ. Poiché $\gamma^2 = d$, questo omomorfismo commuta con il prodotto ed è dunque un omomorfismo di $\mathbb{K}$-algebre.

□

6.3 Applicazione al teorema di Hasse-Minkowski

Le costruzioni presentate in questo capitolo possono essere applicate nella dimostrazione del teorema di Hasse-Minkowski. In particolare, il teorema di Brauer-Hasse-Noether ha come facile conseguenza il caso di una forma quadratica in 3 variabili, mentre gli altri risultati presentati semplificano il passaggio da 3 a 4 variabili. Ciò deriva dall'assumere di aver risolto il primo caso nella maggior generalità in cui il campo su cui è definita la forma sia un qualsiasi campo di numeri $\mathbb{K}$.

Teorema 6.3.1 (Hasse-Minkowski)**.** *Sia q una forma quadratica non degenere in n variabili a coefficienti in $\mathbb{K}$ campo di numeri. Essa ammette vettori isotropi non banali in $\mathbb{K}$ se e solo se ne ammette in $\mathbb{K}_v$ per ogni posto v di $\mathbb{K}$.*

Dimostrazione. La dimostrazione si concentrerà sui casi significativi in cui $n = 3$ e $n = 4$, poiché il caso in più variabili si deduce dai precedenti in modo analogo a quanto visto nel caso $\mathbb{K} = \mathbb{Q}$.

$\boxed{n = 3}$ Posso scrivere la forma senza perdita di generalità come $\langle -a, -b, ab\rangle$. Siano $\mathbb{H} := \mathbb{H}_{\mathbb{K}}(a, b)$ e $\mathbb{H}_v := \mathbb{H} \otimes \mathbb{K}_v = \mathbb{H}_{\mathbb{K}_v}(a, b)$. Per il teorema principale, l'ipotesi che la forma sia isotropa in ogni posto di $\mathbb{K}$ equivale a chiedere che $\mathbb{H}_v \cong M_2(\mathbb{K}_v)$ per ogni v. Dal teorema di Brauer-Hasse-Noether segue in particolare che la mappa i è iniettiva: data un'algebra centrale semplice E su $\mathbb{K}$, se $E \otimes \mathbb{K}_v$ è un'algebra di matrici su $\mathbb{K}_v$ (o equivalentemente rappresenta l'elemento banale del gruppo di Brauer $Br(\mathbb{K}_v)$) per ogni posto v di $\mathbb{K}$, allora anche E è un'algebra di matrici. Applicando questo risultato alle ipotesi, si ha che $\mathbb{H}$ è isomorfa ad un'algebra di matrici, che per questioni di dimensione sarà $M_2(\mathbb{K})$. Per il teorema principale, $\langle -a, -b, ab\rangle$ è isotropa su $\mathbb{K}$.

$\boxed{n = 4}$ Senza perdita di generalità, posso considerare la forma del tipo $\langle 1, -a, -b, c\rangle$ su $\mathbb{K}$. Per ipotesi, la forma è isotropa su ogni $\mathbb{K}_v$, dove v è un posto di $\mathbb{K}$. Sul campo $\mathbb{L} = \mathbb{K}(\sqrt{abc})$ la forma considerata è equivalente a $\langle 1, -a, -b, ab\rangle$: questa è isotropa su tutti i completamenti di $\mathbb{L}$. Sia $\mathbb{H}_{\mathbb{K}} := \mathbb{H}_{\mathbb{K}}(a, b)$ e $\mathbb{H}_{\mathbb{L}} := \mathbb{H}_{\mathbb{K}} \otimes \mathbb{L}$. Per il teorema principale, per ogni completamento $\mathbb{L}_w$ di $\mathbb{L}$, vale che $\mathbb{H}_w := \mathbb{H} \otimes \mathbb{L}_w \cong M_2(\mathbb{L}_w)$, dunque per il caso precedente $\mathbb{H}_{\mathbb{L}} \cong M_2(\mathbb{L})$. Per la proposizione 6.2.4 si ha un'immersione di $\mathbb{K}$-algebre $i : \mathbb{L} \hookrightarrow \mathbb{H}_{\mathbb{K}}$, e la norma di $i(\sqrt{abc}) = xi + yj + zk$ è $-abc = -ax^2 - by^2 + abz^2$, da cui si ricava un vettore isotropo per la forma iniziale, ossia $\left(z, \frac{y}{a}, \frac{x}{b}, 1\right)$.

□

Bibliografia

[Coh07] Henri Cohen. *Number theory. Vol. I. Tools and Diophantine equations*. Vol. 239. Graduate Texts in Mathematics. Springer, New York, 2007, pp. xxiv+650.

[Con] Keith Conrad. *Selmer's example*. URL: `https://kconrad.math.uconn.edu/blurbs/gradnumthy/selmerexample.pdf`.

[Gre83] Gary R. Greenfield. «Sums of three and four integer squares». In: *Rocky Mountain J. Math.* 13.1 (1983), pp. 169–175. ISSN: 0035-7596.

[Hea92] David R. Heath-Brown. «The Density of Zeros of Forms for which Weak Approximation Fails». In: *Mathematics of Computation* (ott. 1992), pp. 613–623.

[IR90] Kenneth Ireland e Michael Rosen. *A classical introduction to modern number theory*. Second. Vol. 84. Graduate Texts in Mathematics. Springer-Verlag, New York, 1990, pp. xiv+389.

[Lin40] Carl-Erik Lind. *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins*. Thesis, University of Uppsala, 1940, p. 97.

[Mil13] James S. Milne. *Class Field Theory (v4.02)*. Available at www.jmilne.org/math/. 2013.

[Rei42] Hans Reichardt. «Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen». In: *J. Reine Angew. Math.* 184 (1942), pp. 12–18.

[Voi18] John Voight. *Quaternion algebras*. 2018, pp. xv+798. URL: `https://math.dartmouth.edu/~jvoight/quat-book.pdf`.