April 8, 2014

TGBD(4) - FORME BILINEARI SIMMETRICHE

1. Nozioni di base e formulazione del problema

Inizialmente R denoterà sia un arbitrario campo $\mathbb{K}$, sia l'anello degli interi $\mathbb{Z}$. In seguito, in vista delle applicazioni topologiche del corso TGBD ci specializzeremo a $\mathbb{K} = \mathbb{Z}/2, \mathbb{R}$.
Consideremo solo *R-modulo liberi finitamente generati*, detti anche $\mathbb{K}$-spazi vettoriali nel caso dei campi. Per definizione un tale modulo V ammette una *base* (ordinata) finita, cioè esiste un sottoinsieme $\mathcal{B} = \{v_1, \dots, v_n\}$ di V che lo genera ed è formato da elementi R-linearmente indipendenti. Fissata una base ordinata $\mathcal{B} = \{v_1, \dots, v_n\}$ di V, si ha l'isomorfismo di passaggio alle coordinate

$$V \to R^n,\ v \to [v]$$

dove R^n indica lo R-modulo libero standard delle matrici con n righe e una colonna con entrate in R; si ha che $[v_i] = e_i$, dove $\mathcal{E} = \{e_1, \dots, e_n\}$ è la base canonica di R^n.

1.1. **Dimensione e rango.** Come gli studenti sanno già dal corso di GAAL, molte proprietà degli spazi vettoriali finitamente generati (tra cui la teoria della dimensione) sono basate su i due teoremi (algoritmi) fondamentali:

- Teorema di *estrazione* di una base ordinata da un qualsiasi insieme finito e ordinato di generatori.
- Teorema di estensione ad una base ordinata di un qualsiasi insieme finito ordinato di vettori linearmente indipendenti.

Entrambi *non* sono veri su $\mathbb{Z}$. Ad esempio, $\mathrm{MCD}(2,3) = 1 = m2 + n3$ (Bezout). Quindi $X = \{2,3\}$ genera $V = \mathbb{Z}$ ma non contiene una base. $X = \{2\}$ è formato da un elemento non nullo quindi linearmente indipendente (perché $\mathbb{Z}$ non ha divisori di zero); ma X non è una base e non si può estendere ad una base (se $m \neq 2$ fosse un altro elemento di questa presunta base allora $m2 + (-2)m = 0$ contro l'indipendenza lineare). Un lemma elementare ma essenziale per la costruzione degli algoritmi che dimostrano i teoremi fondamentali è il seguente:

Se $x_1, \dots x_k$ sono vettori linearmente dipendenti non nulli dello spazio vettoriale V, allora esiste $1 < r \leq k$ tale che $x_r = a_1 x_1 + \dots a_{k-1} x_{k-1}$.

Anche questo non vale su $\mathbb{Z}$. Per esempio non vale per $1, 2$ in $V = \mathbb{Z}$. Ne segue che alcune conseguenze dei teoremi fondamentali valgono anche su $\mathbb{Z}$ ma necessitano una dimostrazione indipendente. Altre conseguenze non valgono. Nel caso degli spazi vettoriali queste sono ben note e rimandiamo a GAAL.

Cominciamo con alcune proprietà che valgono in generale. V denota un R-modulo libero finitamente generato.

Proposizione 1.1. *Due basi di V hanno lo stesso numero di elementi.*

Dim. Su $\mathbb{Z}$: siano $\mathcal{B}$ e $\mathcal{D}$ due basi di V e sia $v \to [v]$ l'isomorfismo di passaggio alle cordinate rispetto a $\mathcal{B}$. Allora l'immagine di $\mathcal{D}$, $[\mathcal{D}]$ è una base di $\mathbb{Z}^n$. Basta dimostrare che qualsiasi base $\mathcal{R}$ di $\mathbb{Z}^n$ ha n elementi. Consideriamo l'estensione naturale di anelli $\mathbb{Z} \subset \mathbb{Q}$, e l'estensione naturale $\mathbb{Z}^n \subset \mathbb{Q}^n$. Basta dimostrare che $\mathcal{R}$ è una base del $\mathbb{Q}$-spazio vettoriale $\mathbb{Q}^n$. Questo segue facilmente dal fatto che per ogni insieme finito $X = \{x_1, \dots, x_r\}$ di vettori di $\mathbb{Q}^n$ esiste un intero d tale che $dX = \{dx_1, \dots, dx_r\} \subset \mathbb{Z}^n$. □

Dunque il numero di elementi di una arbitraria base è un invariante di V che è detto la sua *dimensione* nel caso degli spazi vettoriali e (usualmente) il *rango* di V su $\mathbb{Z}$. Per semplicità, conveniamo di chiamarlo in ogni caso "dimensione".

Proposizione 1.2. *Se W è un sottomodulo di V allora anche W è un R-modulo libero finitamente generato e $\dim W \leq \dim V$.*

Dim. Su $\mathbb{Z}$ è una conseguenza del fatto che $\mathbb{Z}$ è un PID. Sia $\dim V = n$ e $x_1, \dots, x_n$ una base di V. Sia $W_r = W \cap \mathrm{Span}(x_1, \dots, x_r)$. Allora $W_1 = \mathrm{Span}(ax_1)$ per qualche $a \in \mathbb{Z}$. Quindi se non è nullo, W_1 è libero di dimensione uguale a 1. Supponiamo per induzione che l'enunciato valga per W_r e dimostriamo che vale per W_{r+1}. Sia $\mathcal{A} \subset \mathbb{Z}$ formato da tutti gli interi a tale che esiste $x \in W$ della forma

$$x = a_1 x_1 + \dots a_r x_r + a x_{r+1}$$

è chiaro che $\mathcal{A}$ è un ideale di $\mathbb{Z}$, quindi è generato da un elemento a_{r+1}. Se $a_{r+1} = 0$, allora $W_{r+1} = W_r$ e concludiamo per l'ipotesi induttiva. Se $a_{r+1} \neq 0$, sia $w \in W_{r+1}$ il cui coefficiente rispetto a x_{r+1} sia proprio a_{r+1}. Per ogni $x \in W_{r+1}$, il suo coefficiente rispetto a x_{r+1} è divisibile per a_{r+1}, dunque esiste $c \in \mathbb{Z}$ tale che $x - cw \in W_r$. Quindi $W_{r+1} = W_r + \mathrm{Span}(w)$, e chiaramente $W_r \cap \mathrm{Span}(w) = \{0\}$. □

1.2. **Matrici.** Usando gli isomorfismi di passaggio alle coordinate, molte questioni possono essere trattate su R^n in termini di opportune matrici. Indichiamo con $M(n, R)$ la R-algebra delle matrici $n \times n$ con entrate a valori in R. Ogni applicazione R-lineare $f : R^n \to R^n$ è della forma $f(X) = AX$ dove $A \in M(n, R)$ ed è univocamente determinata dalla proprietà che per ogni j, $A^j = f(e_j)$, dove A^j è la j-esima colonna di A. $GL(n, R)$ denota il gruppo moltiplicativo delle matrici invertibili. La matrice $A \in M(n, R)$ è invertibile se e solo se l'applicazione R-lineare $f(X) = AX$ è un isomorfismo. Il *determinante* di A

$$\det(A) = \sum_{\sigma \in S_n} (-1)^{p(\sigma)} a_{1\sigma(1)} \cdots a_{n\sigma(n)}$$

è definito mediante la formula usuale ed ha le proprietà strutturali già viste in GAAL nel caso di $M(n, \mathbb{K})$. Grazie alla formula di Cramer, A è invertibile se e solo se $\det(A) \in R' \subset R$, dove R' è il gruppo moltiplicativo degli elementi invertibili di R. Quindi $R' = R \setminus 0$ se R è un campo, mentre $\mathbb{Z}' = \{\pm 1\}$. Una matrice di $GL(n, \mathbb{Z})$ è anche detta *unimodulare*. Se V è come sopra un R-modulo libero di dimensione $\dim V = n$, le matrici di cambiamento di base di V sono invertibili. Per ogni matrice invertibile $P \in GL(n, R)$, per ogni base $\mathcal{B}$ di V, esistono uniche basi $\mathcal{B}'$, $\mathcal{B}$" di V tali che P è sia la matrice di cambiamento di base $\mathcal{B} \to \mathcal{B}'$, sia di $\mathcal{B}$" $\to \mathcal{B}$.

Vediamo adesso alcuni fatti che valgono in generale (con la stessa dimostrazione).

Proposizione 1.3. *Il modulo duale di V, $V^* := \mathrm{Hom}(V, R)$, è a sua volta libero e $\dim V = \dim V^*$. Infatti, per ogni base $\mathcal{B} = \{v_1, \dots, v_n\}$ di V si ha la base duale $\mathcal{B}^* = \{v_1^*, \dots, v_n^*\}$ di V^*, definita dalle relazioni*

$$v_i^*(v_j) = \delta_{i,j}, \quad i, j = 1, \dots, n \ .$$

E' dato l'accoppiamento bilineare canonico, detto *prodotto di Kronecher*

$$< \cdot, \cdot >: V^* \times V \to R, \quad < v^*, v >= v^*(v) \ .$$

Diciamo che

$$V = \oplus_{j=1}^k W_j$$

è *somma diretta* dei sottomoduli W_j, se ogni $v \in V$ si può scrivere in modo unico nella forma

$$v = \sum_j w_j, \quad w_j \in W_j \ .$$

Equivalentemente, se $\mathcal{B}_j$ è una base di W_j allora $\mathcal{B} = (\mathcal{B}_1, \dots, \mathcal{B}_k)$ è una base di V. Ne segue che $\dim V = \sum_j \dim W_j$. Se $k = 2$, le condizioni precedenti sono equivalenti a $V = W_1 + W_2$ e $W_1 \cap W_2 = \{0\}$. Se V_1 e V_2 sono R-moduli di dimensione n_1 e n_2 rispettivamente, il modulo prodotto $V_1 \times V_2$ ha dimensione $n_1 + n_2$; mediante le inclusioni canoniche $V_1 \to V_1 \times \{0\}$ e $V_2 \to \{0\} \times V_2$, risulta che

$$V_1 \times V_2 = V_1 \oplus V_2 \ .$$

In questo modo abbiamo definito la somma diretta di due R-moduli anche nel caso in cui non sono dati a priori come sottomoduli di uno stesso modulo.

Vediamo infine alcune proprietà che valgono per gli spazi vettoriali ma non su $\mathbb{Z}$.

Proposizione 1.4. *(1) Per ogni sottospazio vettoriale $W \subset V$, se $\dim W = \dim V$, allora $V = W$.*
(2) Per ogni sottospazio vettoriale $W \subset V$, esiste un sottospazio Z di V tale che $V = W \oplus Z$ (diciamo che ogni sottospazio di V è un addendo diretto).

Su $\mathbb{Z}$ consideriamo in particolare il problema di quando $v \in V$, v non nullo, si può estendere ad una base. Sia allora V uno $\mathbb{Z}$-modulo libero, $\dim V = n$. Un elemento $v \in V$ è detto *indivisibile* se non esistono $m \in \mathbb{Z}$ e $v' \in V$ tali che $v = mv'$. Se $[v] \in \mathbb{Z}^n$ è la colonna delle coordinate di V rispetto ad una qualsiasi base, allora v è indivisibile se e solo se il MCD delle coordinate è uguale a 1. Abbiamo il seguente Lemma.

Lemma 1.5. *Un elemento $v \in V$ si estende ad una base di V (equivalentemente,* $\mathrm{Span}(v)$ *è un fattore diretto di V) se e solo se v è indivisibile.*

Dim. Fissiamo una base arbitraria di V e, passando in coordinate, ragioniamo su $\mathbb{Z}^n$, $y = (y_1, \dots, y_n)^t = [v]$. E' evidente che se y non è indivisibile allora non si può estendere ad una base. Per dimostrare l'altra implicazione, dobbiamo far vedere che y è la prima colonna di qualche matrice $D \in GL(n, \mathbb{Z})$. Procediamo per induzione su n. Per $n = 1$ è evidente. Per $n = 2$, l'dentità di Bezout dice che esiste $z = (z_1, z_2)^t \in \mathbb{Z}^2$ tale che $y_1 z_1 + y_2 z_2 = 1$, quindi basta prendere la matrice (y, w) dove $w = (-z_2, z_1)^t$. Se $n > 2$, consideriamo $t = (y_1, \dot{y}_{n-1})$ e sia $d = \mathrm{MCD}(y_1, \dots, y_{n-1})$, $t = dt'$, dove t' è indivisibile. Dunque per induzione esiste una matrice unimodulare $(n-1) \times (n-1)$ D' che ha t' come prima colonna e quindi una matrice intera D_{n-1} che ha t come prima colonna e $\det D_{n-1} = d$. Si ha che

$$\mathrm{MCD}(d, y_n) = 1$$

quindi (Bezout) esistono interi p e q tali che $pd - qy_n = 1$. Poniamo allora D_n la matrice intera $n \times n$ che ha come ultima riga $(y_n, 0, \dots, 0, p)$, come ultima colonna $(\frac{y_1 q}{d}, \dots, \frac{y_{n-1} q}{d}, p)$, mentre il minore $(n-1) \times (n-1)$ di D_n ottenuto eliminando l'ultima riga e l'ultima colonna è uguale a D_{n-1}. Sviluppando il determinante rispetto all'ultima riga si verifica che $\det D_n = 1$.

□

Ricordiamo anche il seguente risultato di struttura degli $\mathbb{Z}$-moduli finitamente generati. Dato un tale modulo E, non nevessariamente libero, $T(E)$ indica il sottomodulo di *torsione* di E, formato dagli elementi $x \in E$ tali che esiste $a \in \mathbb{Z}$, $ax = 0$. Allora :

$T(E)$ è finito. Il modulo quoziente $F = E/T(E)$ è libero. E è isomorfo a $T(E) \oplus F$. In particolare E è libero se e solo se $T(E) = \{0\}$.

1.3. **Forme bilineari simmetriche.** Al solito sia V un R-modulo libero di dimensione finita, $\dim V = n$. Una forma R-bilineare su V

$$\Phi : V \times V \to R$$

è simmetrica (è una FBS) se per ogni $v, w \in V$, si ha che

$$\Phi(v, w) = \Phi(w, v) \ .$$

Se W è un sottomodulo di V, Φ si restringe ad una FBS su W.
Associata a Φ abbiamo l'applicazione R-lineare canonica

$$F = F_\Phi : V \to V^*, \quad F(v)(w) = \Phi(v, w) \ .$$

La FBS Φ è detta *non singolare* se F è un isomorfismo.
Due FBS Φ e Ψ su V e W rispettivamente si dicono *isometriche* se esiste un isomorfismo R-lineare $f : V \to W$ tale che, per ogni $v, w \in V$,

$$\Phi(v, w) = \Psi(f(v), f(w)) \ .$$

Il problema principale che vogliamo affrontare è la *classificazione delle FBS non singolari a meno di isometrie* per $R = \mathbb{R}, \mathbb{Z}/2, \mathbb{Z}$. Ci restringiamo a questi anelli particolari in vista delle applicazioni topologiche fatte nel corso di TGBD. Poiché per ogni isomorfismo lineare $V \to (W, \Psi)$, la FBS su V definita da $\Phi(v, w) = \Psi(f(v), f(w))$ è tautologicamente isometrica a Ψ, è equivalente studiare a meno di isometrie le FBS su un dato V. Quindi:

Da ora in poi stipuliamo che $R = \mathbb{R}, \mathbb{Z}/2, \mathbb{Z}$.

Per $\mathbb{R}$ la cosa è già stata trattata in GAAL, come caso particolare dello studio dei prodotti scalare (sinomimo di FBS) sugli spazi vettoriali di dimensione finita, avendo fatto l'ipotesi restrittiva che il campo $\mathbb{K}$ degli scalari è di caratteristica $\neq 2$, cioè $2 = 1 + 1 \neq 0$. Quindi $\mathbb{Z}/2$ va considerato a parte perché è di caratteristica 2, $\mathbb{Z}$ perché non è un campo.

1.4. **Formulazione matriciale.** Sia Φ una FBS su V, $\dim V = n$. Date una base $\mathcal{B} = \{v_1, \dots, v_n\}$ di V e la base duale $\mathcal{B}^*$ di V^*, si ha che

$$F(v_i) = \sum_j m_{ij} v_j^*, \quad m_{ij} = \phi(v_i, v_j)$$

e la matrice simmetrica

$$M = M_{\mathcal{B}}(\Phi), \quad M = (m_{ij})$$

è detta la matrice che rappresenta Φ rispetto ala base $\mathcal{B}$. Si ha che per ogni $v, w \in V$

$$\Phi(v, w) = [v]^t M [w] \ .$$

La seguente proposizione vale in tutti i casi con la stessa dimostrazione.

Proposizione 1.6. *(1) M e N sono matrici simmetriche che rappresentano la FBS Φ rispetto a due basi diverse di V se e solo se sono* congruenti *cioè esiste $P \in GL(n, R)$ tale che*

$$N = P^t M P \ .$$

(2) M e N sono matrici simmetriche che rappresentano due FBS Φ e Ψ isometriche rispetto ad una stessa base di V, se e solo se sono congruenti.
(3) Una FBS Φ su V è non singolare se e solo se una matrice simmetrica M che rappresenta Φ è invertibile. In tal caso tutte le matrici simmetriche che rappresentano Φ sono invertibili.

Quindi la versione matriciale del nostro problema consiste nella classificazione delle matrici simmetriche invertibili di $M(n, R)$ a meno della relazione di congruenza.

2. Decomposizioni in somma diretta-ortogonale

I risultati di questa sezione valgono, con la stessa dimostrazione, per ogni $R = \mathbb{R}, \mathbb{Z}/2, \ \mathbb{Z}$. Sia V munito della FBS non singolare Φ. Sia W un sottomodulo di V. Allora

$$W^\perp = \{v \in V |\ \Phi(v, w) = 0, \ \forall w \in W\}$$

è il sottomodulo di V *ortogonale* a W. La notazione

$$V = W_1 \perp \cdots \perp W_k$$

significa che

$$V = W_1 \oplus \cdots \oplus W_k$$

ed inoltre, per ogni $i \neq j$, $W_i \subset W_j^\perp$. In tal caso si dice che abbiamo una decomposizione in somma diretta-ortogonale di (V, Φ). Necessariamente la restrizione di Φ ad ogni W_j è non singolare. Se (V_1, Φ_1) e (V_2, Φ_2) sono R-moduli di dimensione n_1 e n_2 risperrivamente, muniti di FBS non singolari, il modulo prodotto $V = V_1 \times V_2 = V_1 \oplus V_2$ è munito di un unica FBS non singolare Φ tale che

$$(V, \Phi) = (V_1, \Phi_1) \perp (V_2, \Phi_2) \ .$$

Proposizione 2.1. *(1) Sia W un sottomodulo di V tale che la restrizione di Φ su W è non singolare. Allora*

$$V = W \perp W^\perp$$

(2) Se $X = \{x_1, \dots, \ x_k\} \subset V$ è tale che la matrice simmetrica $k \times k$, $M = (\Phi(x_i, x_j)$ è invertibile, allora X è una base di $W := \mathrm{Span}(X)$ e $V = W \perp W^\perp$.
(3) Esiste una decomposizione di (V, Φ) della forma $V = U_1 \perp \dots U_k \perp N$, dove $\dim U_i = 1$ per ogni $i = 1, \dots, k$, mentre per ogni $x \in N$, $\Phi(x, x)$ non è un elemento invertibile di R.

Dim. (1) Se $w \in W \cap W^{\perp}$, allora $\Phi(w', w) = 0$ per ogni $w' \in W$, dunque $w = 0$ perché la restrizione di Φ su W è non singolare. Resta così da dimostrare che $V = W + W^{\perp}$. Per ogni $v \in V$ si consideri la restizione su W della forma lineare $F(v)$, $w \to \Phi(v, w)$. Poiché la restrizione di Φ è non singolare, esiste un unico $w' \in W$ tale per $F(v)(w) = \Phi(w', w)$. Quindi $v - w' \in W^{\perp}$ e $v = w' + (v - w')$. Il punto (1) è così dimostrato.
(2) Gli elementi di X sono linearmente indipendenti, perché una qualsiasi relazione lineare non banale $a_1x_1 + \cdots + a_kx_k = 0$ implicherebbe l'annullamento del determinante della matrice $M = (\Phi(x_i, x_j)$. Il resto è una conseguenza del punto (1).
(3) Se esiste $v \in V$ tale che $\Phi(v, v) \in R$ è invertibile, allora grazie al punto (1) si ha che $V = \mathrm{Span(v)} \perp \mathrm{Span(v)}^{\perp}$. Si conclude in modo induttivo in un numero finito di passi (perché la dimensione cala ad ogni passo).

□

3. Classificazione delle FBS su $\mathbb{R}$

Una proprietà fondamentale delle FBS su $\mathbb{R}$ (più in generale su ogni campo di caratteristica $\neq 2$) è che

Φ *è nulla se e solo se per ogni* $v \in V$, $\Phi(v, v) = 0$ *(cioè tutti i vettori di* V *sono isotropi).*

Questa è una conseguenza della formula di "polarizzazione"

$$2\Phi(v, w) = \Phi(v + w, v + w) - \Phi(v, v) - \Phi(w, w) \ .$$

Dunque la Proposizione 2.1 ha come corollario ("esistenza di basi ortogonali") che:

$$V = U_1 \perp \ldots U_k \ .$$

Su $\mathbb{R}$, se Ψ è non degenere su U, $\dim U = 1$ e v è una base, allora $\Phi(av, av) = a^2\Phi(v, v)$, quindi Ψ è definita (positiva o negativa) su U. Per l'esistenza della radice quadrata di ogni reale positivo, si può normalizzare la base in modo che $\Phi(v_j, v_j) = \pm 1$. Infine (Teorema di Sylvester) il numero i_+ (i_-) di addendi definiti positivi (negativi) non dipende dalla decomposizione; infatti i_+ detto *indice di positività* è uguale alla massima dimensione realizzata dai sottospazi di V tali che la restrizione di Φ è definita positiva. Analogamente per l' *indice di negatività* i_-. Chiaramente la coppia

$$(i_+, i_-)$$

è un invariante completo e $i_+ + i_- = n = \dim V$. A meno di isometrie si ha la decomposizione in forma normale (con l'ovvio significato della notazione):

$$(V, \Phi) = i_+U_+ \perp i_-U_- \ .$$

3.1. Decomposizione di Witt.

La *segnatura* di Φ è definita da

$$\sigma := i_+ - i_-$$

e chiaramente anche la coppia (σ, n) è un invariante completo. La segnatura governa in modo più diretto un'altra decomposizione canonica, detta di Witt. Premettiamo una definizione che vale per ogni R. $H = (W, \Psi)$ è un *piano iperbolico* se $\dim W = 2$ ed esiste una base $\mathcal{D}$ di W (detta una base iperbolica di H) rispetto alla quale Ψ è rappresentata dalla matrice

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

(V, Φ) ammette allora una decomposizione (unica a meno di isometrie di (V, Φ)) della forma

$$V = A \perp \mathcal{H}$$

dove:

(1)
$$\dim A = |\sigma|$$
e la restrizione di Φ su A è definita, di segno uguale al segno di σ.

(2)
$$\mathcal{H} = \frac{n-|\sigma|}{2} H$$
cioè è una somma diretta-ortogonale di piani iperbolici.

Osservazioni 3.1. (1) $U_- \perp U_+$ è un piano iperbolico.
(2) Su $\mathbb{R}$ (più in generale su ogni campo di caratteristica $\neq 2$), $H = (W, \Psi)$ è un piano iperbolico se e solo se $\dim W = 2$, Φ è non singolare ed esiste $w \in W$, $w \neq 0$, tale che $\Psi(w, w) = 0$. Inoltre, per ogni tale vettore isotropo non nullo w esiste una base iperbolica di H della forma $\mathcal{D} = \{w, t\}$.
(3) Su $\mathbb{R}$, Φ è definita (positiva o negativa) se e solo se è *anisotropa* (cioè $v = 0$ è il solo vettore isotropo). La decomposizione canonica di Witt esiste su ogni campo di caratteristica $\neq 2$, dove in generale A è da intendersi anisotropo.
(4) L'invariante $\frac{n-|\sigma|}{2}$ (più in generale il numero di piani iperbolici nella decomposizione di Witt) è noto anche come *indice di Witt* ed è uguale alla massima dimensione che si realizza al variare di Z tra i sottospazi di V tali che la restrizione di Φ è nulla. Si osserva che per ogni tale Z, $Z = Z^\perp$.

4. Classificazione delle FBS su $\mathbb{Z}/2$

Osserviamo subito che, contrariamente al caso precedente, un piano iperbolico su $\mathbb{Z}/2$ è *totalmente isotropo*, cioè per ogni $v \in H$, $\Psi(v, v) = 0$. Inoltre è evidente che a meno di isometrie esiste un unico $U = (U, \Psi)$ non singolare di dimensione uguale a 1. Possiamo enunciare la classificazione.

Proposizione 4.1. *(1) Se* $\dim V = n = 2m + 1$*, allora esiste una decomposizione canonica (unica a meno di isometrie) della forma*
$$(V, \Phi) = nU \ .$$
(2) Se $\dim V = n = 2m$*, allora si hanno le due seguenti possibilità (che si escludono a vicenda)*

- *Esiste una decomposizione canonica (unica a meno di isometrie) della forma*
$$(V, \Phi) = nU \ .$$
- *Esiste una decomposizione canonica (unica a meno di isometrie) della forma*
$$(V, \Phi) = mH \ .$$

Dim. I tre casi sono distinti l'uno dall'altro dalla dimensione o da essere o no totalmente isotropi. Per dimostrare l'esistenza di queste decomposizioni, partiamo da una decomposizione come in (3) della Proposizione 2.1:
$$(V, \Phi) = kU \perp N$$
dove ora N è totalmente isotropo. Mostriamo che se $N \neq \{0\}$, allora
$$N = sH, \ 2s + k = n \ .$$
Basta dimostrare che N contiene un piano iperbolico H, perché poi si può concludere per induzione sulla dimensione, applicando (1) della Proposizione 2.1. Sia $w \in N$, $w \neq 0$. Poichè $\mathbb{Z}/2$ è un campo, possiamo estendere w ad una base $\mathcal{D} = \{w = v_1, \ldots, v_r\}$ di N. Sia $\mathcal{D}^*$ la base duale. Poiché $\Phi|N$ è non singolare, esiste un unico $t \in \mathbb{N}$ tale che, per ogni $x \in N$, $v_1^*(x) = \Phi(t, x)$. Si verifica allora che $\mathrm{Span}(\{w, t\})$ è un piano iperbolico (munito della base iperbolica $\{w, t\}$). Per terminare la dimostrazione della Proposizione, basta ora dimostrare che
$$U \perp H = 3U \ .$$
Sia $\mathcal{D} = \{u, w, t\}$ una base di $U \perp H$ adattata alla decomposizione e tale che $\{w, t\}$ sia una base iperbolica di H. Consideriamo $T = (\mathrm{Span}(\{u + w, u + t\}), \Phi|)$. Si verifica direttamente che
$$T = 2U$$
munito della base ortogonale $\{u + w, u + t\}$. Applicando il punto (1) della proposizione Proposizione 2.1, si conclude che
$$U \perp H = T \perp T^\perp = 3U \ .$$
□

Osservazioni 4.2. (1) Su $\mathbb{R}$ (più in generale su ogni campo di caratteristica $\neq 2$), vale il *Teorema di cancellazione di Witt*:

Se $W \perp Z$ è isometrico a $W' \perp Z$, allora W e W' sono isometrici.

Questo non è più vero su $\mathbb{Z}/2$, infatti abbiamo visto sopra che $U \perp H$ è isometrico a $U \perp (2U)$, ma H e $2U$ non sono isometrici.
(2) Le forme normali del teorema di classificazione possono essere equivalentemente riscritte come segue:

$$U \perp (2mU),\ 2mU,\ \ mH\ \ .$$

Gli addendi del tipo $2mU$, mH hanno in comune la seguente proprietà

Hanno dimensione pari $2m$ ed esiste un sottospazio Z, $\dim Z = m$ tale che $Z = Z^{\perp}$

In generale (per ogni R) chiamiamo *neutro* un (W, Ψ) che verifica queste proprietà. Non è difficile dimostrare, usando argomenti simili a quelli già usati che:

Proposizione 4.3. *(1) Su ogni campo $\mathbb{K}$ di caratteristica $\neq 2$, (W, Ψ) è neutro se e solo se*

$$(W, \Psi) = mH\ .$$

(2) su $\mathbb{Z}/2$, (W, Ψ) è neutro se e solo se ammette una delle due decomposizioni

$$(W, \Psi) = 2mU,\ (W, \Psi) = mH\ .$$

Dunque la riscrittura messa in evidenza sopra può essere considerata come una estensione su $\mathbb{Z}/2$ della forma normale di Witt.

5. Classificazione delle FBS intere unimodulari

La trattazione è parecchio più complessa che nei casi precedenti e non darà luogo ad un risultato completo.
Sottoclassi invarianti. E' conveniente rispartire le FBS unimodulari in diverse sottoclassi invarianti rispetto alle isometrie (cioè due forme isometriche appartengono alla stessa sottoclasse).

- Diciamo che la FBS unimodulare Φ su V è *definita* (rispettivamente positiva o negativa) se per ogni $v \in V$, $v \neq 0$, si ha che $\Phi(v, v) > 0$, rispettivamente $\Phi(v, v) < 0$. Altrimenti diciamo che la forma è *indefinita*.
- Diciamo che Φ è *pari* se per ogni $v \in V$, si ha che $\Phi(v, v) \in 2\mathbb{Z}$. Altrimenti diciamo che la forma è *dispari*.

Combinando queste condizioni abbiamo una partizione in sottoclassi più fine.
Il seguente Lemma è una semplice conseguenza della formula di polarizzazione.

Lemma 5.1. *Φ è pari se e solo se esiste una base $\mathcal{B} = \{v_j\}$ di V tale che per ogni j, $\Phi(v_j, v_j)$ è pari. In tal caso questo vale per ogni base di V.*

La segnatura. Grazie all'estensione dei coefficienti $\mathbb{Z} \subset \mathbb{R}$, due matrici simmetriche congruenti su $\mathbb{Z}$ lo sono su $\mathbb{R}$, quindi è ben definita la loro *segnatura* σ che è quindi un invariante delle FBS intere unimodulari a meno di isometrie su $\mathbb{Z}$. La segnatura è additiva rispetto alla somma diretta-ortogonale.

5.1. **Reticoli in $\mathbb{R}^n$.** Sia $A \in GL(n, \mathbb{R})$. Le colonne A^j di A (considerate come elementi di $\mathbb{R}^n$) generano un sottogruppo L di $(\mathbb{R}^n, +)$, detto un *reticolo di* $\mathbb{R}^n$. Il quoziente $\mathbb{R}^n/L$ è un n-toro "piatto" (diffeomorfo a $(S^1)^n$). Un *dominio fondamentale* di L in $\mathbb{R}^n$ è dato da

$$D = \{\sum_j a_j A^j |\ a_j \in \mathbb{R},\ 0 \leq \sum_j a_j < 1\}\ .$$

Il volume del toro (rispetto alla misura indotta dalla metrica euclidea su $\mathbb{R}^n$) è uguale al volume di D e quindi

$$\mathrm{Vol}(\mathbb{R}^n/L) = \mathrm{Vol}(D) = |d| = |\det A|\ .$$

Abbiamo il seguente (caso particolare di un) teorema di Minkowski.

Proposizione 5.2. *Sia $D(r)$ la palla chiusa di $\mathbb{R}^n$ di centro 0, raggio r e volume uguale a $\omega_n r^n$ ($\omega_1 = 2,\ \omega_2 = \pi,\ \omega_3 = \frac{4}{3}\pi,\ \omega_4 = \frac{\pi^2}{2},\ \dots$). Sia L un reticolo di $\mathbb{R}^n$. Se $\omega_n r^n \geq 2^n \mathrm{Vol}(\mathbb{R}^n/L)$, allora esiste un elemento non nullo di L che appartiene a $D(r)$.*

Dim. Dimostriamo intanto il risultato se $\omega_n r^n > 2^n \mathrm{Vol}(\mathbb{R}^n/L)$. In tal caso si ha che $\mathrm{Vol}(D(r/2)) > \mathrm{Vol}(\mathbb{R}^n/L))$. Quindi la restrizione a $D(r/2)$ della proiezione naturale $\mathbb{R}^n \to \mathbb{R}^n/L$ (che è una isometria locale) non può essere iniettiva. Dunque esistono due punti distinti $x, y \in D(r)$ tali che $\frac{x-y}{2} \in L$. Ma quest'ultimo punto non nullo è il punto di mezzo del segmento $[x, -y]$ che è contenuto in $D(r)$ perché è simmetrico rispetto a 0 e convesso. Questo dimostra che se $\omega_n r^n \geq 2^n \mathrm{Vol}(\mathbb{R}^n/L)$, allora per ogni $\epsilon > 0$, esiste un elemento non nullo di L contenuto in $D(r+\epsilon)$. Per compattezza di $D(r+\epsilon)$ l'insieme dei punti non nulli di L contenuti in $D(r+\epsilon)$ è finito, quindi quello più vicino all'origine appartiene necessariamente a $D(r)$.

□

Corollario 5.3. *Sia Φ una FBS unimodulare su V, $\dim V = n$. Allora esiste $v \in V$, $v \neq 0$, tale che $|\Phi(v,v)| \leq 4/(\omega_n)^{2/n}$.*

Dim. Fissiamo una base $\mathcal{B}$ di V e rappresentiamo Φ per mezzo della matrice simmetrica unimodulare A. Quindi, per ogni $v \in V$, $\Phi(v,v) = [v]^t A[v]$. A definisce un prodotto scalare su $\mathbb{R}^n$. Esiste $P \in GL(n,\mathbb{R})$ tale che $A = P^t D P$ dove D è diagonale e ogni elemento sulla diagonale è uguale a ± 1. Poiché $\pm 1 = \det A = \det D \det(P^2)$ ne segue che $\det P = \pm 1$. Se $PB = A$, allora le colonne B^j di B generano un reticolo L di $\mathbb{R}^n$ tale $\mathbb{R}^n/L$ ha volume uguale a 1. Applicando il teorema di Minkowski, esiste $x \in L$ non nullo tale che

$$x^t x \leq 4/(\omega_n)^{2/n}\ .$$

Per costruzione Px ha coordinate intere, così che esiste $v \in V$ tale che $x = [v]$. Risulta infine che

$$|\Phi(v,v)| = |x^t D x| \leq 4/(\omega_n)^{2/n}\ .$$

□

5.2. **Classificazione completa per $\dim V \leq 4$.** Il seguente è un Corollario immediato di quello precedente, basta verificare infatti che se $n \leq 4$ allora $4/(\omega_n)^{2/n} < 2$.

Corollario 5.4. *Sia Φ una FBS unimodulare su V, $\dim V = n \leq 4$. Allora esiste $v \in V$, $v \neq 0$, tale che $|\Phi(v,v)| < 2$.*

Possiamo infine enunciare la classificazione

Proposizione 5.5. *Sia Φ una FBS unimodulare su V, $\dim V = n \leq 4$, $\sigma(\Phi) = \sigma$ di segno ϵ. Allora si realizza una e una sola delle seguenti possibilità*

(1) (V,Φ) *ammette una base ortogonale, cioè si decompone in somma diretta-ortogonale delle forma*
$$|\sigma| U_\epsilon \perp \frac{n-|\sigma|}{2}(U_+ \perp U_-)$$
(2) $(V,\Phi) = H$.
(3) $(V,\Phi) = 2H$. *Negli ultimi due casi la forma è pari e la segnatura $\sigma = 0$.*

Dim. E' banalmente vero quando $n = 1$.
Supponiamo $n = 2$. Per il corollario precedente ci sono due possibiltà. Esiste $v \in V$ non nullo tale che $\Phi(v,v) = \pm 1$, oppure $\Phi(v,v) = 0$. Nel primo caso, applicando il punto (1) della Proposizione 2.1, si ha che $(V,\Phi) = U_\pm \perp U_\epsilon$, $\epsilon = \pm$. Nel secondo caso possiamo supporre che v sia indivisibile. Dunque si può estendere ad una base $\{v, w\}$ di V. Se $t \in V$ è tale che per ogni $x \in V$ si ha che $\Phi(t,x) = v^*(x)$, anche $\{v,t\}$ è una base. Se la forma è pari (cioè se $\Phi(t,t) = a$ è pari) allora $\{v, t - \frac{1}{2}av\}$ è una base iperbolica di V. Se la forma è dispari (cioè se $\Phi(t,t) = a = 2k+1$) allora $\{v' = t - kv, t' = t - (k+1)v\}$ è una base ortogonale di V corrispondente alla decomposizione $(V,\Phi) = U_+ \perp U_-$.

Supponiamo $n = 3$. Ragionando come nel caso precedente si vede che ci sono a priori due possibilità: (V, Φ) ammette una base ortogonale, oppure

$$(V, \Phi) = H \perp U_{\pm} \ .$$

Mostriamo che in effetti anche nel secondo caso esiste una base ortogonale. Sia $\{v, t, u\}$ una base adattata formata da una base iperbolica di H e da una base normalizzata di $U_{\pm}$. Poniamo $T = \mathrm{Span}(\{v, t + u\})$; la restrizione di Φ a T è non singolare e rientra nel secondo caso visto prima per $n = 2$. Quindi

$$(V, \Phi) = T \perp U_{\epsilon} = U_{+} \perp U_{-} \perp U_{\epsilon} \ .$$

Supponiamo $n = 4$. Ragionando in modo simile si vede che si hanno due possibilità: la forma è dispari e quindi ammette una base ortogonale, oppure è pari e $(V, \Phi) = 2H$.

□

5.3. **Teorema di Meyer.** E' il risultato chiave per la classificazione delle FBS intere unimodulari indefinite.

Proposizione 5.6. *Se Φ è una FBS intera unimodulare indefinita su V, allora esiste $v \in V$ non nullo tale che $\Phi(v, v)) = 0$*

Se $n = \dim V \leq 4$ è una conseguenza della classificazione già ottenuta. Per $n \geq 5$ ci limiteremo a indicare i punti essenziali della dimostrazione, che si basa su risultati classici e profondi di teoria dei numeri. Il lettore interessato piuttosto alle applicazioni può andare direttamente alla sezione successiva.

Fissiamo una base di V e trattiamo la questione in coordinate. Sia $\mathbb{Z}^n \subset \mathbb{Q}^n$ e $A \in GL(n, \mathbb{Z})$ che rappresenta Φ. A definisce un prodotto scalare su $\mathbb{Q}^n$ e basta dimostrare che esiste $x \in \mathbb{Q}^n$ non nullo tale che $x^t Ax = 0$. Siamo cioè ricondotti a dimostrare che (come succede per $\mathbb{R}$), su $\mathbb{Q}$ in dimensione $n \geq 5$ ogni prodotto scalare è anisotropo se e solo se è definito. Si noti che per $n \leq 4$ non è vero; per esempio l'equazione $y_1^2 + y_2^2 + y_3^2 - 7y_4^2$ non ha soluzioni intere (e quindi non ne ha razionali) come si può verificare considerando la sua riduzione mod(8). Il nostro prodotto scalare ammette comunque una base ortogonale su $\mathbb{Q}$. Cambiando coordinate ci siamo ridotti a dimostrare che ogni equazione del tipo

$$a_1 y_1^2 + \cdots + a_5 y_5^2 = 0$$

dove i coefficienti $a_j \in \mathbb{Q}$, sono non nulli e non hanno tutti lo stesso segno ha una soluzione non nulla in $\mathbb{Q}^5$. Grazie al *Teorema di Hasse-Minkowsi*, sappiamo che la nostra equazione ha soluzioni razionali se e solo se ha soluzioni in ogni estensione p-adica $\mathbb{Q}_p$ di $\mathbb{Q}$. Vale il seguente fatto:

- Sia p un primo dispari, u, v, w elementi invertibili dell'anello degli interi p-adici $\mathbb{Z}_p$. Allora l'equazione $uy_1^2 + vy_2^2 + wy_3^2 = 0$ ha una soluzione non nulla in $\mathbb{Z}_p$.

Indichiamo come si conclude la dimostrazione. Se p è dispari, ogni coefficiente a_i dell'equazione può essere sia invertibile in $\mathbb{Q}_p$ sia p volte un elemento invertibile. Quindi ci sono due possibilità: almeno tre coefficienti sono invertibili o almeno tre sono p volte elementi invertibili. In ogni caso si applica il fatto enunciato qui sopra e si conclude. Se $p = 2$, condizione necessaria affinché un elemento di $\mathbb{Z}_2$ sia un quadrato è che sia congruo a 1 mod(8). Possiamo assumere, a meno di permutare i coefficienti e moltiplicare per una costante, che a_1, a_2 e a_3 siano unità di $\mathbb{Z}_2$, mentre a_4 e a_5 sono al più divisibili per 2. Si verifica allora per ispezione diretta che la congruenza

$$a_2 y_1^2 + \cdots + a_5 y_5^2 \equiv -1 \ \mathrm{mod}(8)$$

ha soluzioni e si può concludere in modo simile al caso di p dispari.

□

6. Classificazione delle forme unimodulari indefinite dispari

Abbiamo

Proposizione 6.1. *Sia Φ unimodulare indefinita dispari su V, $\dim V = n$, $\sigma(\Phi) = \sigma$ di segno ϵ. Allora (V, Φ) ammette una base ortogonale, cioè si decompone in somma diretta-ortogonale delle forma*

$$|\sigma| U_\epsilon \perp \frac{n - |\sigma|}{2}(U_+ \perp U_-) \ .$$

Dim. Procediamo per induzione su n. Il risultato è già noto per $n \leq 4$. Grazie al Teorema di Meyer, sia $v \in V$ non nullo e tale che $\Phi(v, v) = 0$. Ragionando come nella dimostrazione della proposizione 5.5, possiamo supporre che v sia indivisibile e che esista quindi una base $y_1, \ldots, y_n$ tale che tale che $\Phi(v, y_1) = 1$. Almeno uno degli y_k è tale che $\Phi(y_k, y_k)$ è dispari. Se si tratta di y_1, consideriamo $T = \mathrm{Span}(\{v, y_1\})$. Se $\Phi(y_1, y_1)$ è pari prendiamo $T = \mathrm{Span}(\{v, y_1 + y_k\})$. Abbiamo visto che allora $T = U_+ \perp U_-$, quindi $(V, \Phi) = U_+ \perp U_- \perp T^\perp$. Almeno un $\epsilon = \pm$ è tale che $U_\epsilon \perp T^\perp$ è indefinita e dispari e si conclude per induzione.

□

7. Congruenze modulo 8

Sia come al solito una FBS unimodulare su V, $\dim V = n$. Diciamo che $u \in V$ è un *elemento caratteristico* se per ogni $v \in V$ si ha che

$$\Phi(u, v) \equiv \Phi(v, v) \mathrm{mod}(2) \ .$$

Abbiamo il seguente Lemma di van der Blij.

Lemma 7.1. *(1) Esistono sempre elementi caratteristici.*
(2) Per ogni elemento caratteristico u, $\sigma(\Phi) \equiv \Phi(u, u)$ mod(8).

Dim. (1) Fissiamo una base di V e la matrice A che rappresenta Φ. Condideriamo il prodotto scalare su $(\mathbb{Z}/2)^n$ indotto dalla riduzione mod 2 $\bar{A}$ di A. La funzione $(\mathbb{Z}/2)^n \to \mathbb{Z}/2$ definita da $\bar{x} \to \bar{x}^t \bar{A} x$ è $\mathbb{Z}/2$-lineare; quindi esiste un unico $\bar{u} \in (\mathbb{Z}/2)^n$ tale che per ogni $\bar{x}$, $\bar{u}^t \bar{A} x = \bar{x}^t \bar{A} x$. Ogni $u \in \mathbb{Z}^n$ tale che la sua riduzione mod (2) è uguale a $\bar{u}$ è un elemento caratteristico cercato.
(2) Siano u e u' due elementi caratteristici; allora $u' = u + 2x$ per qualche x. Quindi $\Phi(u', u') = \Phi(u, u) + 4(\Phi(u, x) + \Phi(x, x)) \equiv \Phi(u, u)$ mod (8). Questo invariante mod (8) è additivo rispetto alle somme dirette-ortogonali. Vale ± 1 per $U_\pm$. Usando la classificazione segue che il punto (2) è vero per le forme indefinite e dispari. La segnatura di un arbitrario (V, Φ) è uguale alla segnatura di $(V, \Phi) \perp U_+ \perp U_-$ e quest'ultimo è indefinito e dispari. Il Lemma è così dimostrato.

□

Corollario 7.2. *Se (V, Φ) è pari allora $\sigma(\Phi) \equiv 0$ mod(8).*

Dim. In questo caso $u = 0$ è caratteristico.

□

8. Classificazione delle forme unimodulari indefinite pari

Un Corollario della classificazione delle forme indefinite dispari su V è che due tali forme sono isometriche se e solo se hanno la stessa segnatura. Vogliamo estendere questo risultato alle forme indefinite pari.

Proposizione 8.1. *Due FBS unimodulari indefinite e pari Φ, Ψ su V sono isometriche se e solo se hanno la stessa segnatura.*

Dim. Supponiamo che abbiano la stessa segnatura. Poiché sono indefinite e pari, utilizzando il lemma di Meyer come già fatto nel caso dispari, si ottiene che

$$(V, \Phi) = Y \perp H, \ (V, \Psi) = Y' \perp H$$

dove Y e Y' sono pari e hanno la stessa segnatura. Poniamo $W = U_+ \perp U_-$ munito di una base ortonormale adattata e_1, e_2, e consideriamo $X = Y \perp W$, $X' = Y' \perp W$ muniti delle naturali FBS somma-diretta-ortogonale. Questi sono dispari ed hanno la stessa segnatura, quindi coincidono a meno di isometria. Vogliamo determinare in X e X' dei sottomoduli Z e Z' tra loro isometrici e che

risulteranno essere isometrici rispettivamente a $Y \perp H$ e $Y' \perp H$. Questo concluderà la dimostrazione. Posto genericamente $T = X, X', W$ e indicata con β la FBS su T, applichiamo a $(T\beta)$ la seguente costruzione. Sia T_0 il sottomodulo di indice 2 di T formato dagli elementi $x \in T$ pari, cioè tali che

$$\beta(x, x) \equiv 0 \mathrm{mod}(2) \ .$$

Consideriamo il $\mathbb{Q}$-spazio vettoriale $\mathbb{Q} \otimes T$, associato all'estensione dei coefficienti $\mathbb{Z} \subset \mathbb{Q}$. Quindi $T \subset \mathbb{Q} \otimes T$ ed ogni base di T è una base di $\mathbb{Q} \otimes T$ su $\mathbb{Q}$. La forma β si estende su $\mathbb{Q} \otimes T$. Sia $T_0^\bullet$ il sottogruppo di $(\mathbb{Q} \otimes T, +)$ formato dagli $x^\bullet \in \mathbb{Q} \otimes T$ tali che

$$\beta(x^\bullet, x) \in \mathbb{Z}$$

per ogni $x \in T_0$. Chiaramente $T_0 \subset T_0^\bullet$. Si verifica direttamente che:

(1) Gli elementi $e_1 + e_2, e_1 - e_2$ formano una base di $W_0^\bullet$.
(2) Ci sono esattamente 3 sottomoduli che contengono propriamente W_0 e sono propriamente contenuti in $W_0^\bullet$: uno di questi è W, gli altri due sono isometrici a H.
(3) $X_0 = Y \perp W_0$, $X_0^\bullet = Y \perp W_0^\bullet$.
(4) Ci sono esattamente tre sottomoduli che contengono propriamente X_0 e sono propriamente contenuti in $X_0^\bullet$: uno uno di questi è X, gli altri due sono entrambi isometrici a $Y \perp H$. A meno di isometria denotiamoli con Z. Le stesse considerazioni ci portano a definire Z' isometrico a $Y' \perp H$.

E' chiaro dalla costruzione che, a meno di isometria, Z dipende solo dalla classe di isometria di X. Poiché X e X' sono isometrici, si conclude che Z e Z' sono isometrici.

□

8.1. **Forme normali.** Indichiamo con $E_8 = (\mathbb{Z}^8, \beta)$ dove $\beta(x, y) = x^t E y$ e $E = (e_{i,j}$ è la matrice simmetrica definita come segue:

- $e_{i,i} = 2$ per ogni i;
- $e_{i,i+1} = 1$ per $i = 1, \ldots, 6$;
- $e_{5,8} = 1$;
- $e_{i,j} = 0$ altrimenti.

Si verica con calcoli diretti che E_8 è unimodulare, pari, definita positiva (per esempio usando il criterio di Jacobi). Quindi la sua segnatura $\sigma(E_8) = 8$. $-E_8 = (\mathbb{Z}^n, -\beta)$ è pari, definita negativa con segnatura $\sigma = -8$. Tenendo conto sia della congruenza mod(8) verificata dalla segnatura, sia della Proposizione precedente abbiamo il seguente corollario

Corollario 8.2. *Sia (V, Φ), $n = \dim V$, tale che la FBS Φ è unimodulare, indefinita e pari. Allora (a meno di isometria)*

$$(V, \Phi) = aE_8 \perp bH$$

dove $a = \dfrac{\sigma}{8}$ *e* $b = \dfrac{n - |\sigma|}{2}$.

Segue dalla discussione precedente che

Corollario 8.3. *(1) (V, Φ) indefinito e dispari è neutro se e solo se $(V, \Phi) = m(U_+ \perp U_-)$.*
(2) (V, Φ) indefinito e pari è neutro se e solo se $(V, \Phi) = mH$.

Quindi le forme normali così ottenute per le FBS indefinite (pari o dispari) sono la versione su $\mathbb{Z}$ della *decomposizione di Witt.*

9. Cenni sulle forme unimodulari definite

Queste non sono classificate. Ci limitiamo a ricordare in proposito alcuni risultati qualitativi. Non è restrittivo limitarci a considerare il caso definito positivo.

Lavorando in coordinate, ogni matrice simmetrica intera unimodulare M definisce un prodotto scalare β su $\mathbb{R}^n$, via l'estensione dei coefficienti $\mathbb{Z} \subset \mathbb{R}$. Se M è definita positiva, esiste $P \in GL(n, \mathbb{R})$ tale che $M = P^t P$. Le colonne di P generano un reticolo L di R^n. Questo $\mathbb{Z}$-modulo libero L munito della

restrizione del prodotto scalare euclideo standard su $\mathbb{R}^n$ è isometrico a $(\mathbb{Z}^n, \beta|)$. Quindi $\mathrm{Vol}(\mathbb{R}^n/L) = 1$. Abbiamo così dimostrato:

Lemma 9.1. *Ogni $\mathbb{Z}$-modulo libero V di dimensione n, munito di una FBS unimodulare definita positiva è isometrico ad un reticolo L di $\mathbb{R}^n$, di volume uguale a 1, munito della FBS indotta dal prodotto scalare euclideo standard di $\mathbb{R}^n$ (diremo che un tale L, non necessariamente di volume unitario, è un reticolo euclideo).*

Per esempio E_8 si realizza come reticolo euclideo per mezzo del reticolo $\Gamma_8 \subset \mathbb{R}^8$ (di volume 1) generato dai vettori della forma $e_i + e_j$, $i \neq j$, e $\frac{1}{2}(e_1 + \cdots + e_8)$. Analogamente, per ogni $4m$ si può definire il reticolo di volume 1, $\Gamma_{4m} \subset \mathbb{R}^{4m}$.

Abbiamo il seguente risultato di finitezza

Proposizione 9.2. *Per ogni $n \geq 1$ ed ogni reale $d > 0$, esiste un numero finito di classi di isometria di reticoli euclidei in $\mathbb{R}^n$ di volume uguale a d.*

Corollario 9.3. *Per ogni $n \geq 1$, esiste un numero finito di classi di isometria di FBS unimodulari definite (positive) di dimensione uguale a n.*

Diamo un cenno della dimostrazione della Proposizione. Procediamo per induzione su n. Per $n = 1$ è banale. Sia L un reticolo euclideo in $\mathbb{R}^n$ di volume uguale a d. Per il teorema di Minkowski esiste una costante $c(n, d)$ tale che L contiene un x non nullo tale che $x^t x \leq c(n, d)$. Sia L^0 il sottoreticolo di L formato dai punti $y \in L$ tali che

$$x^t y \equiv 0, \ \mathrm{mod}(x^t x) \ .$$

L^0 ha indice finito r in L, $r \leq c(n, d)$, $\mathrm{Vol}(L^0) = r\mathrm{Vol}(L) \leq c(d, n)d$. L^0 si decompone in somma ortogonale del sottoreticolo generato da x e del reticolo complementare ortogonale L'. Per induzione, a meno di isometrie, esiste un numero finito di possibilità per L', quindi per L^0 e quindi per L.

□

(V, Φ) con Φ definita positiva è detta *indecomponibile* se non può essere decomposto in modo non banale in somma diretta-ortogonale di sottomoduli. Per esempio, E_8 è indecomponibile. Vale il seguente Teorema di Eichler.

Proposizione 9.4. *Ogni (V, Φ), con Φ unimodulare definita positiva, si decompone in modo unico (a meno di isometrie) in somma diretta-ortogonale di sottomoduli indecomponibili.*

Dim. Un elemento x di V si dice minimale se non può essere scritto nella forma $x = y + z$ con $\Phi(y, y), \Phi(z, z) < \Phi(x, x)$. Gli elementi minimali generano V. Se $V = X \perp X'$, allora ogni elemento minimale appartiene ad uno dei due addendi diretti. Diciamo che due elementi minimali x, x' sono equivalenti se esiste una sequenza finita di elementi minimali, $x = x_0, x_1, \ldots, x_k = x'$ tale che $\Phi(x_{i-1}, x_i) \neq 0$. Ogni classe di equivalenza genera un sottomodulo di V e V è la somma diretta-ortogonale di questi sottomoduli. Questa decomposizione è univocamente determinata. □

Osservazioni 9.5. (1) Il numero delle classi di isometria delle FBS unimodulari definite positive cresce molto rapidamente con la dimensione, anche restringendosi alle forme pari. Ponendo $c(n8)$ il numero di queste ultime classi relative alla dimensione $8n$, abbiamo $c(8) = 1$, $c(16) = 2$, $c(24) = 24$, $c(32) \geq 10^7$, $c(40) \geq 10^5 1 \ldots$.
(2) Lo studio delle forme unimodulari definite positive è anche collegato con il classico problema di determinare gli "impacchettamenti di palle" di massima densità. Un tale impacchettamento in $\mathbb{R}^n$ è una unione di palle di raggio uguale r con parti interne disgiunte. Ogni reticolo euclideo L ha associato un impacchettamento, dove le palle hanno centro nei punti del reticolo e il raggio $r = \min_{x \in L \setminus \{0\}} x^t x$.

10. Il gruppo di Witt

Consideriamo $\mathcal{I}(R)$ l'insieme delle classi di isometria di FBS non singolari definite su R-moduli liberi di dimensione finita arbitraria. Questo è un semigruppo commutativo mediante l'operazione di somma diretta-ortogonale $\perp$. Mettiamo su $\mathcal{I}(R)$ la seguente relazione di equivalenza:

$X \cong X'$ se e solo se esistono S e S' neutri tali che $X \perp S = X' \perp S'$.

Denotiamo con $\mathcal{W}(R)$ l'insieme quoziente. Se $X = [(V, \beta)]$, indichiamo con $-X = [(V, -\beta)]$. Segue dalla discussione precedente che per ogni $R = \mathbb{R}, \mathbb{Z}/2, \mathbb{Z}$, per ogni X, $-X \perp X$ è neutro. Dunque l'operazione $\perp$ discende su $\mathcal{W}(R)$ e lo rende un gruppo abeliano, con elemento neutro dato dalla classe degli X neutri. Questo è detto il *gruppo di Witt di R*. Su $\mathbb{Z}$, se restringiamo tutto il discorso alle forme pari, definiamo in modo analogo il gruppo di Witt $\mathcal{W}_0(\mathbb{Z})$. Analogamente su $\mathbb{Z}/2$ otteniamo $\mathcal{W}_0(\mathbb{Z}/2)$ restringendoci alle forme totalmente isotrope. La seguente Proposizione è una conseguenza immediata dei risultati di classificazione ottenuti nelle sezioni precedenti.

Proposizione 10.1. *(1) Per $R = \mathbb{R}, \mathbb{Z}$ la segnatura definisce un isomorfismo di gruppi*

$$\sigma : \mathcal{W}(R) \to (\mathbb{Z}, +) \ .$$

(2)

$$\frac{\sigma}{8} : \mathcal{W}_0(\mathbb{Z}) \to (\mathbb{Z}, +)$$

è un isomorfismo di gruppi.
(3)

$$r_2 : \mathcal{W}(\mathbb{Z}/2) \to \mathbb{Z}/2$$

dove $r_2([(V, \beta)]) = [\dim V]$ mod(2), è un isomorfismo di gruppi.
(4) $\mathcal{W}_0(\mathbb{Z}/2) = 0$.

11. Forme quadratiche

Sia come al solito V un R-modulo libero, $\dim V = n$. Una *forma quadratica su V* è per definizione una funzione

$$q : V \to R$$

tale che:

- Per ogni $a \in R$, per ogni $x \in V$, $q(ax) = a^2(x)$;
- L'applicazione $\phi_q : V \times V \to \mathbb{R}$ definita da

$$\phi_q(x, y) = q(x + y) - q(x) - q(y)$$

è una FBS.

Se β è una forma bilineare su V, non necessariamente simmetrica, allora

$$q(x) := q_\beta(x) = \beta(x, x)$$

definisce una forma quadratica e

$$\phi_q(x, y) = \beta(x, y) + \beta(y, x) \ .$$

Se $\beta = \phi$ è simmetrica, allora

$$\phi_{q_\phi} = 2\phi \ .$$

Quindi su $\mathbb{R}$ (più in generale su ogni campo di caratteristica $\neq 2$)

$$q \to \phi_q, \ \phi \to \frac{1}{2} q_\phi$$

definiscono una bigezione canonica tra le forme quadratiche e le FBS. Su R arbitrario, ogni forma quadratica q si può realizzare nella forma $q = q_\beta$ per qualche FB β, in generale non simmetrica. Se $q_\beta = q_{\beta'}$, allora $\alpha = \beta - \beta'$ è *simplettica*), cioè $\alpha(x, x) = 0$ per ogni $x \in V$, quindi α è *antisimmetrica*, cioè $\alpha(x, y) = -\alpha(y, x)$.
Su $\mathbb{Z}$ una FBS del tipo ϕ_q è pari: $\phi_q(x, x) = 4q(x) - 2q(x) = 2q(x)$. Su $\mathbb{Z}/2$ è totalmente isotropa. Su $\mathbb{Z}/2$, una forma del tipo q_ϕ è lineare.

11.1. $\mathbb{Z}/2$**-Forme quadratiche a valori in** $\mathbb{Z}/4$**.** Per le applicazioni topologiche del corso di TGBD, siamo più che altro interessati al caso di $\mathbb{Z}/2$ ed a una generalizzazione della nozione di forma quadratica.
Ricordiamo che esiste un' immersione canonica di $(\mathbb{Z}/2,+)$ in $(\mathbb{Z}/4,+)$

$$2 : \mathbb{Z}/2 \to \mathbb{Z}/4,\ 2[n]_2 := [2n]_4 \ .$$

Sia allora (V,ϕ) uno $\mathbb{Z}/2$-spazio vettoriale, $\dim V = n$, munito della FBS non singolare ϕ. Per definizione una *forma quadratica su* (V,ϕ) *a valori in* $\mathbb{Z}/4$ è una funzione

$$q : V \to \mathbb{Z}/4$$

tale che

$$q(x+y) = q(x) + q(y) + 2\phi(x,y) \ .$$

Si osserva immediatamente che $q(0) = q(0+0) = q(0) + q(0) + 2\phi(0,0) = q(0) + q(0)$, da cui $q(0) = 0$.

Osservazioni 11.1. Se $\bar{q} : V \to \mathbb{Z}/2$ è una forma quadratica ordinaria, allora $q = 2\bar{q}$ è quadratica a valori in $\mathbb{Z}/4$ su (V,ϕ_q). D'altra parte, se ϕ è totalmente isotropa, allora una forma quadratica $q : (V,\phi) \to \mathbb{Z}/4$ è a valori in $2\mathbb{Z}/2$; dunque $q = 2\bar{q}$, dove $\bar{q} : V \to \mathbb{Z}/2$ è una forma quadratica ordinaria. Queste osservazioni mostrano che stiamo effettivamente considerando una generalizzazione delle forme quadratiche ordinarie.

Esiste una naturale nozione di isomorfismo tra terne (V,ϕ,q). (V,ϕ,q) e (V',ϕ,q') si dicono isomorfi se esiste una isometria

$$f : (V,\phi) \to (V',\phi')$$

tale che

$$q'(f(x)) = q(x)$$

per ogni $x \in V$. Si definisce in modo usuale l'operazione di somma diretta

$$(V_1,\phi_1,q_1) \perp (V_2,\psi_2,q_2)$$

e questa operazione passa al livello della classi di isomorfismo $\mathcal{IQ}(\mathbb{Z}/2,\mathbb{Z}/4)$, che ha quindi una struttura di semigruppo. Per allegerire la notazione, a volte scriveremo semplicemente q, $q_1 \perp q_2$, ... sottoindendendo la struttura completa (V,ϕ,q), $(V_1,\phi_1,q_1) \perp (V_2,\psi_2,q_2)$ ... . Spesso confonderemo anche le classi di isomorfismo con un loro rappresentante.
Possiamo definire il *gruppo di Witt* in questo contesto, ripetendo parola per parola la costruzione già vista prima. Diciamo (V,ϕ,q) è *neutro* se (V,Φ) è neutro ed esiste un sottospazio Z di V tale che $Z = Z^{\perp}$ e q si annulla su Z. Anche questa nozione passa al livello delle classi di isomorfismo. Per ogni q, $-q \perp q$ è neutro. Diciamo che q e q' sono equivalenti se esistono s e s' neutre tali che

$$q \perp s = q' \perp s' \ .$$

Allora la struttura di semigruppo di $\mathcal{IQ}(\mathbb{Z}/2,\mathbb{Z}/4)$ discende sul quoziente, definendo il gruppo di Witt in questione:

$$\mathcal{WQ}(\mathbb{Z}/2,\mathbb{Z}/4) \ .$$

Vogliamo determinare $\mathcal{WQ}(\mathbb{Z}/2,\mathbb{Z}/2))$.

11.2. **L'invariante di Arf-Brown.** Indichiamo con $U_8 \subset \mathbb{C}$ il gruppo moltiplicativo delle radici ottave di 1. Fissiamo anche l'isomorfismo

$$\epsilon : (\mathbb{Z}/8,+) \to U_8,\ \epsilon(1) = \exp(\frac{i\pi}{4}) \ .$$

Per ogni forma quadratica $q : (V,\phi) \to \mathbb{Z}/4$, per ogni $x \in V$ poniamo

$$f(x) = \exp(\frac{i\pi q(X)}{2}) = i^{q(x)}$$

$$\gamma(q) = (\frac{1}{\sqrt{2}})^n \sum_{x \in V} f(x) \ .$$

Chiaramente γ è un invariante a meno di isomorfismo, dunque definisce un'applicazione

$$\gamma : \mathcal{I}Q(\mathbb{Z}/2, \mathbb{Z}/4) \to \mathbb{C}$$

Vogliamo dimostrare:

Proposizione 11.2. *L'applicazione γ è a valori in U_8, passa al quoziente ed induce un isomorfismo di gruppi*

$$\gamma : \mathcal{W}Q(\mathbb{Z}/2, \mathbb{Z}/4) \to U_8$$

la cui versione additiva è

$$\alpha : \mathcal{W}Q(\mathbb{Z}/2, \mathbb{Z}/4) \to (\mathbb{Z}/8, +),\ \gamma = \epsilon \circ \alpha\ .$$

Dim. Cominciamo analizzando le possibili forme quadratiche a valori in $\mathbb{Z}/4$, sullo spazio elementare U di dimensione 1 (che è munito di un unica FBS non singolare). Sia $q : U \to \mathbb{Z}/4$. Allora $0 = q(1+1) = 2q(1) + 2$, da cui $q(1) = \pm 1$ e ci sono dunque due forme quadratiche q_+ e q_- su U.

Utilizzando la classificazione delle FBS su $\mathbb{Z}/2$, sappiamo che ogni

$$(V, \phi) \perp 2U = aU$$

dunque ogni

$$(V, \phi, q) \perp q_+ \perp q_- = rq_+ \perp sq_-$$

per qualche $r + s = a$. Poiché $q_+ \perp q_-$ è neutro, ne seque che $\mathcal{W}Q(\mathbb{Z}/2, \mathbb{Z}/4)$ è ciclico, generato da q_+.

Dimostriamo adesso che $4q_+$ è isomorfa a $4q_-$, da cui segue che $8q_+ = 4q_+ \perp 4q_-$ è neutro. Infatti, siano $g_j : U \to 4U,\ j = 1, \ldots, 4,\ g_1(x) = (0, x, x, x),\ g_2(x) = (x, 0, x, x),\ g_3(x, x, 0, x),\ g_4(x) = (x, x, x, 0)$. Poiché $4q_+(g_j(x)) = 3q_+(x) = q_-(x)$ e $g_i(U)$ e $g_j(U)$ sono ortogonali se $i \neq j$, si ha che $(g_1, g_2, g_3, g_4) : 4U \to 4U$ è l'isomorfismo cercato. Ne segue che l'ordine del gruppo ciclico $\mathcal{W}Q(\mathbb{Z}/2, \mathbb{Z}/4)$ divide 8.

Consideriamo ora l'applicazione $\gamma : \mathcal{I}Q(\mathbb{Z}/2, \mathbb{Z}/4) \to \mathbb{C}$. Affermiamo che è *moltiplicativa*, cioè

$$\gamma(q_1 \perp q_2) = \gamma(q_1)\gamma(q_2)\ .$$

Infatti

$$\gamma(q_1 \perp q_2) = (\frac{1}{\sqrt{2}})^{n_1+n_2} \sum_{x \in V_1, y \in V_2} i^{q_1(x)} i^{q_2(y)} =$$

$$[(\frac{1}{\sqrt{2}})^{n_1} \sum_{x \in V_1} i^{q_1(x)}][(\frac{1}{\sqrt{2}})^{n_2} \sum_{y \in V_2} i^{q_2(y)}] = \gamma(q_1)\gamma(q_2)\ .$$

Osserviamo che $\gamma(q_+) = \exp(\frac{i\pi}{4})$ (radice ottava primitiva di 1), $\gamma(q_-) = \exp(\frac{-i\pi}{4})$, quindi $\gamma(q_+ \perp q_-) = 1$. Ne segue che per ogni $q \in \mathcal{I}Q(\mathbb{Z}/2, \mathbb{Z}/4)$

$$\gamma(q) = \gamma(q \perp q_+ \perp q_-) = \gamma(q_+)^r \gamma(q_-)^s \in U_8\ .$$

Per dimostrare che γ passa al quoziente bisogna dimostrare che per ogni q neutra, si ha che $\gamma(q) = 1$, come abbiamo già verificato direttamente nel caso particolare della forma neutra $q_+ \perp q_-$. Segue anche dalla discussione precedente che $\gamma(8q_+) = 1$. Sia allora q neutra. Ragionando come prima si ha che

$$\gamma(q) = \gamma(q \perp q_+ \perp q_-) = \gamma(q_+)^r \gamma(q_-)^s$$

con l'informazione ulteriore che adesso $rU \perp sU$ è neutro per cui, per esempio, sappiamo che $r+s = 2m$ è pari. Vogliamo dimostrare che in effetti $r = s$. Non è restrittivo supporre che $r, s \leq 7$. Poniamo $\tilde{q} := rq_+ \perp sq_-$ su $rU \perp sU := W_+ \perp W_-$, munito della base ortogonale adattata $e_1, \ldots, e_r, f_1, \ldots, f_s$. Supponiamo per assurdo che $r > s$, cioè $r = m+k,\ 1 \leq k$. Quindi le coppie (r, k) che a priori dobbiamo considerare e che dobbiamo potere escludere sono $(3,1)$, $(4,1)$, $(5,1)$, $(5,2)$, $(6,1)$, $(6,2)$, $(7,1)$,$(7,2)$, $(7,3)$. Sia Z un sottospazio vettoriale di $W_+ \perp W_-$ tale che $\dim Z = m$, $Z = Z^\perp$, $\tilde{q}|Z = 0$. Per la formula di Grassmann, $\dim(Z \cap W_+) = k$. Descriviamo gli elementi non nulli v di $W_+ \perp W_-$ tali che $\tilde{q}(v) = 0$. Se $v \in W_\pm$ allora v è la somma di quattro elementi distinti della base di $W_\pm$. Altrimenti

v è la somma di due j-uple di elementi distinti delle due basi di W_+ e W_- (cioè della forma $e_h + f_h$, $e_h + e_s + f_h + f_t$, ecc.). Possiamo subito escludere $(3,1)$ perché W_+ non contiene alcun elemento non nullo v tale che $\tilde{q}(v) = 0$. Nel caso $(4,1)$, $W_+ \cap Z \setminus \{0\}$ consiste necessariamente dell'unico vettore $e_1 + e_2 + e_3 + e_4$. Gli unici vettori $v \in W_+ \perp W_-$ tali che $\tilde{q}(v) = 0$ e $\tilde{q}(e_1 + e_2 + e_3 + e_4 + v) = 0$ sono della forma $e_h + e_s + f_1 + f_2$. Due vettori di questo tipo v, v' sono tali che $\tilde{q}(v + v') = 0$ se e solo se $v + v' = e_1 + e_2 + e_3 + e_4$. Dunque un sottospazio totalmente isotropo di $W_+ \perp W_-$ che contiene $e_1 + e_2 + e_3 + e_4$ ha al più dimensione uguale a 2, mentre Z avrebbe dimensione uguale a 3. Dunque anche $(4,1)$ è escluso. Nel caso $r = 5$, consideriamo due vettori distinti della forma $v = e_{j_1} + \cdots + e_{j_4}$, $v' = e_{l_1} + \cdots + e_{l_1}$. In ogni caso $\tilde{q}(v + v') \neq 0$, quindi un sottospazio di W_+ totalmente isotropo ha dimensione al più uguale a 1. Quindi $(5,2)$ è escluso. Nel caso $(5,1)$, a meno di riordinare le basi, possiamo assumere che $Z \cap W_+ \setminus \{0\}$ consista dell'unico vettore $e_1 + e_2 + e_3 + e_4$. I vettori non nulli v non contenuti in W_+ tali che $\tilde{q}(v) = 0$ e $\tilde{q}(e_1 + e_2 + e_3 + e_4 + v) = 0$ sono della forma $v = e_h + e_s + f_i + f_j$, $h, s \in \{1,2,3,4\}$. Supponiamo ad esempio che un sottospazio totalmente isotropo contenga $e_1 + e_2 + e_3 + e_4$ e $e_1 + e_2 + f_1 + f_2$; allora ha dimensione al più uguale a 3, ed un esempio tipico ha per base $e_1 + e_2 + e_3 + e_4, e_1 + e_2 + f_1 + f_2, e_1 + e_3 + f_1 + f_3$. Dunque anche $(5,1)$ è escuso perché Z dovrebbe avere dimensione uguale a 4. Gli altri casi si trattano con argomenti simili. Dunque abbiamo verificato che γ passa al quoziente: $\gamma : \mathcal{WQ}(\mathbb{Z}/2, \mathbb{Z}/4) \to U_8$.

A questo punto possiamo concludere: il gruppo di Witt è ciclico, generato da q_+ di ordine un divisore di 8. $\mathrm{Im}(\gamma)$ è generata da $\gamma(q_+)$ che è una radice ottava primitiva di 1. Quindi γ è un isomorfismo.

□

Osservazioni 11.3. (1) L' invariante moltiplicativo $\gamma(q)$ è detto l'*invariante di Arf-Brown*. Se la FBS associata a q è totalmente isotropa, così che $q = 2\bar{q}$, dove $\bar{q}$ è una forma quadratica ordinaria, allora f prende solo i valori ± 1. In questo caso $\gamma(q)$ coincide con il più classico invariante di Arf di $\bar{q}$ che vale $+1$ se la forma prende più spesso il valore 0 che il valore 1, -1 nel caso contrario.
(2) Usando gli argomenti precedenti, si può mostrare che l'invariante di Arf-Brown insieme alla dimensione di V e al carattere (non) totalmente isotropo della FBS associata, formano un insieme completo di invarianti di isomorfismo.
(3) Si può dare una dimostrazione più sintetica del fatto che $\gamma(q) = 1$ quando q è neutra, che indichiamo qui sotto:

Sia $Z \subset V$ tale che $Z = Z^\perp$ e q si annulla su Z. Fissiamo una decomposizione in somma diretta (non ortogonale) $V = Z \oplus L$. Per ogni $x \in L$ non nullo, si consideri la forma lineare $\rho : Z \to \mathbb{Z}/2$, $\rho(z) = \phi(x, z)$. Poiché ϕ è non singolare e $Z = Z^\perp$, segue che $\dim \mathrm{Ker}(\rho) = \dim Z - 1$, dunque $|\rho^{-1}(0)| = |\rho^{-1}(1)|$. Se $\dim V = n$, calcoliamo

$$\gamma(q) = (\frac{1}{\sqrt{2}})^n \sum_{z \in Z, x \in L} f(z + x) = (\frac{1}{\sqrt{2}})^n \sum_{z \in Z, x \in L} f(x)(-1)^{\phi(x,z)} =$$

$$(\frac{1}{\sqrt{2}})^n [\sum_{x \neq 0} (\sum_{z \in Z} (-1)^{\phi(x,z)} f(x)) + |Z|] = (\frac{1}{\sqrt{2}})^n |Z| = (\frac{1}{\sqrt{2}})^n (2^{n/2}) = 1 \ .$$