Riv. Mat. Univ. Parma (2) 6 (1965), 169-223

CAHIT ARF e GIACOMO SABAN (*)

Due dimostrazioni elementari del teorema di Cartan e Dieudonné. (**)

Introduzione.

0. – Un noto teorema, dovuto ad ELIE CARTAN [1], permette di affermare che *il gruppo dei movimenti di uno spazio euclideo o pseudo-euclideo reale o complesso coincide con il gruppo generato dalle simmetrie rispetto ad iperpiani* (non perpendicolari ad una direzione isotropa) *di questo spazio.*

Di questo teorema si è avuta un'estensione ad opera di J. DIEUDONNÉ [2], che è conseguente a certi lavori di WITT [3] e di ARF [4], e nella quale si dimostra che il teorema enunciato sopra vale anche se lo spazio è definito sopra un campo qualunque, eccezion fatta di un particolare spazio di dimensione quattro che verrà meglio specificato nel seguito.

Sono note varie dimostrazioni di questo teorema [5]: ciò non di meno la presente esposizione non appare superflua sia perchè le due dimostrazioni che ne fanno l'oggetto sono, a nostra conoscenza, originali, sia ancora perchè permettono di giungere alla conclusione mediante l'impiego di nozioni del tutto elementari.

(*) Indirizzo; Centro Nucleare Ricerca Addestramento di Çekmece, P.K.1 - Hava Alani, Istanbul, Turchia.

(**) La presente pubblicazione costituisce l'oggetto del Report No. ÇNAEM-17 (1964) del Centro Nucleare di Ricerca e Addestramento di Çekmece. L'argomento è stato esposto da G. SABAN al Sem. Mat. Univ. Parma il 25 e 28 febbraio 1964. Una prima parte è apparsa precedentemente in dispense dell'Ist. Mat. Univ. Roma (G. SABAN, *Introduzione alla Teoria algebrica degli Spinori*, Parte 1ª, Roma 1963). — Ricevuto il 27-X-1964.

1. – Sia V uno spazio vettoriale di dimensione finita, definito sopra un campo K, e si consideri una applicazione $B(\boldsymbol{x}, \boldsymbol{y})$ $(\boldsymbol{x}, \boldsymbol{y} \in V)$ (1) di $V \times V$ in K che sia lineare in ciascuno degli argomenti di B: si dice in tal caso che B è una *forma bilineare* definita su V (2).

Una forma bilineare è *simmetrica* se $B(\boldsymbol{x}, \boldsymbol{y}) = B(\boldsymbol{y}, \boldsymbol{x})$, *alternante* se $B(\boldsymbol{x}, \boldsymbol{y}) + B(\boldsymbol{y}, \boldsymbol{x}) = 0$.

Si osservi che se K ha *caratteristica* 2 ogni forma alternante è pure simmetrica. Nel seguito verranno considerate solamente forme bilineari dotate di queste proprietà.

Scelto un qualsivoglia spazio vettoriale U in V, il sotto-spazio vettoriale

$$U^0 = \{ \boldsymbol{x} \in V \mid B(\boldsymbol{x}, \boldsymbol{y}) = 0 \text{ per } \forall \boldsymbol{y} \in U \} \subset V$$

si chiama *spazio coniugato* di U ed una forma bilineare B definita su V è detta *non degenere* se $V^0 = \{ 0 \}$.

Si dimostra facilmente che

a) $(L + M)^0 = L^0 \cap M^0$;

b) $(L \cap M)^0 = L^0 + M^0$;

c) Se $L \supseteq M$, si ha $M^0 \subseteq L^0$;

d) Se B è non degenere, si ha $(L^0)^0 = L$.

Un sottospazio vettoriale I di V è detto *isotropo* se $I \cap I^0 \neq \{ 0 \}$, e *totalmente isotropo* quando $I \subseteq I^0$.

2. – Si consideri ora una applicazione $Q(\boldsymbol{x})$ di V in K tale che

a) $Q(a\boldsymbol{x}) = a^2 Q(\boldsymbol{x})$;

b) $B(\boldsymbol{x}, \boldsymbol{y}) = Q(\boldsymbol{x} + \boldsymbol{y}) - Q(\boldsymbol{x}) - Q(\boldsymbol{y})$ sia una forma bilineare su $V \times V$; a questa applicazione si dà il nome di *forma quadratica* su V e si verifica imme-

---

(1) Nel seguito verranno stampati in grassetto gli elementi dello spazio vettoriale V ed in corsivo gli elementi del campo K. Per 0, elemento di V, e per 0, elemento di K, si addotterà il medesimo carattere.

(2) La *bilinearità* notoriamente si esprime mediante le seguenti formule:

$$B(\boldsymbol{x}_1 + \boldsymbol{x}_2, \boldsymbol{y}) = B(\boldsymbol{x}_1, \boldsymbol{y}) + B(\boldsymbol{x}_2, \boldsymbol{y}), \qquad B(\boldsymbol{x}, \boldsymbol{y}_1 + \boldsymbol{y}_2) = B(\boldsymbol{x}, \boldsymbol{y}_1) + B(\boldsymbol{x}, \boldsymbol{y}_2),$$

$$B(a\boldsymbol{x}, \boldsymbol{y}) = a\, B(\boldsymbol{x}, \boldsymbol{y}), \qquad B(\boldsymbol{x}, b\boldsymbol{y}) = b\, B(\boldsymbol{x}, \boldsymbol{y}),$$

ove $\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{x}, \boldsymbol{y} \in V$; $a, b \in K$.

diatamente che la forma bilineare B (*associata* alla forma quadratica) è sempre simmetrica ed inoltre, se K ha caratteristica 2, è anche alternante, come risulta dalla formula

$$B(\boldsymbol{x}, \boldsymbol{y}) + B(\boldsymbol{y}, \boldsymbol{x}) = 2[Q(\boldsymbol{x} + \boldsymbol{y}) - Q(\boldsymbol{x}) - Q(\boldsymbol{y})] = 0,$$

che è conseguenza immediata della definizione. Infine una forma quadratica viene detta *non degenere* qualora sia non degenere la forma bilineare ad essa associata.

Si chiama *totalmente singolare* ogni sottospazio S di V tale che sia $Q(\boldsymbol{x}) = 0$ per $\forall \boldsymbol{x} \in S$; si chiama ancora *elemento singolare* ogni elemento di V tale che $\boldsymbol{s} \neq 0$, $Q(\boldsymbol{s}) = 0$.

Dalla definizione di forma quadratica Q e di forma bilineare B ad essa associata segue che ogni sottospazio totalmente singolare in V è sempre totalmente isotropo in V, mentre ogni sottospazio totalmente isotropo di V è totalmente singolare in V *purchè* K abbia una caratteristica diversa da 2.

Due elementi $\boldsymbol{x}$ ed $\boldsymbol{y}$ di V sono detti *ortogonali* se $B(\boldsymbol{x}, \boldsymbol{y}) = 0$.

Il numero minimo di generatori dello spazio vettoriale V definito su K viene chiamato *dimensione* dello spazio considerato ed indicato con $\dim_K V$: nel seguito si considereranno principalmente spazi vettoriali di dimensioni finita e ad un qualsiasi sistema minimale di generatori di questo spazio si darà il nome di *base* di V. Si dimostra facilmente che se il campo K sul quale è definito V ha caratteristica diversa da due, V ha sempre una base composta da vettori mutuamente ortogonali. Inoltre, se B è non degenere e $\dim_K V = n$, $\dim_K R = r$, con $R \subset V$, $r < n$, si dimostra che $\dim_K R^0 = n - r$.

3. – Poste le definizioni che precedono, si può dimostrare il seguente

Teorema 1. *Se V è uno spazio vettoriale definito sul campo K, B una forma bilineare non degenere definita su V ed U uno spazio vettoriale contenuto in V tale che $\dim_K U = r$ con r finito, si ha*

$$\dim_K (V \text{ modulo } U^0) = \dim_K U .$$

Dimostrazione. Osserviamo anzitutto che poichè $\dim_K U = r < \infty$, lo spazio vettoriale U è dotato di base: sia quindi $(\boldsymbol{e}_i)_{i \in (1,r)}$ una qualsiasi base di U. Se esiste una famiglia libera di elementi $(\boldsymbol{\epsilon}_i)_{i \in (1,r)}$ di V tali che sussistano le relazioni

$$B(\boldsymbol{e}_i, \boldsymbol{\epsilon}_j) = \delta_{ij}, \qquad i, j \in (1, r), \tag{1}$$

allora:

1°) detto x un qualsiasi elemento di V,

$$x^0 = x - \sum_{i\in(1,r)} B(x,\ e_i)\ \epsilon_i \in U^0,$$

poichè la condizione di appartenenza di un vettore u_0 ad U^0 si scrive

$$B(u_0,\ e_i) = 0\ , \qquad i \in (1,\ r)\ , \tag{2}$$

e questo sistema di condizioni è identicamente verificato dal vettore x^0, per via delle (1);

2°) $u^* = \sum_{i\in(1,r)} \lambda_i\ \epsilon_i \in U^0$ implica $\lambda_i = 0$, $i \in (1,\ r)$, come immediatamente risulta scrivendo il sistema (2) per il vettore u^*;

3°) dalle due osservazioni preliminari precedenti segue che lo spazio

$$U^* = \bigoplus_{i\in(1,r)} K\epsilon_i$$

è tale che

$$\dim_K U^* = r, \qquad U^* \cap U^0 = \{0\},$$

e quindi

$$V = U^* \oplus U^0. \tag{3}$$

Quest'ultima relazione dimostra l'asserto.

Per completare la dimostrazione è quindi sufficiente mostrare l'effettiva esistenza di una famiglia libera $(\epsilon_i)_{i\in(1,r)}$ soddisfacente le (1). Si procederà per induzione, supponendo esistente una famiglia libera

$$(\epsilon_\mu)_{\mu\in(1,s)}, \qquad 0 \leqslant s < r\ , \tag{4}$$

tale che

$$B(e_\nu,\ \epsilon_\mu) = \delta_{\nu\mu}, \qquad \nu,\ \mu \in (1,\ s)\ .$$

Si consideri allora, assieme allo spazio

$$\widetilde{U}_s = \bigoplus_{\nu\in(1,s)} Ke_\nu,$$

lo spazio $\widetilde{U}_s^0$ ad esso coniugato e si supponga sia

$$B(\boldsymbol{e}_{s+1},\ \boldsymbol{x}') = 0 \qquad \text{per } \forall \boldsymbol{x}' \in \widetilde{U}_s^0 . \tag{5}$$

Allora, posto

$$\boldsymbol{e}_{s+1}^* = \boldsymbol{e}_{s+1} - \sum_{\nu \in (1,s)} B(\boldsymbol{e}_{s+1},\ \boldsymbol{\epsilon}_\nu)\, \boldsymbol{e}_\nu ,$$

si verifica immediatamente che

$$B(\boldsymbol{e}_{s+1}^*,\ \boldsymbol{x}') = 0 .$$

Inoltre, se

$$U_s^* = \bigoplus_{\nu \in (1,s)} K \boldsymbol{\epsilon}_\nu ,$$

il ragionamento che ha condotto alla (3) permette di concludere che

$$V = \widetilde{U}_s^* + \widetilde{U}_s^0 ,$$

e quindi ogni $\boldsymbol{x} \in V$ si scriverà

$$\boldsymbol{x} = \boldsymbol{x}' + \sum_{\nu \in (1,s)} \xi_\nu\, \boldsymbol{\epsilon}_\nu ,$$

essendo $\boldsymbol{x}'$ un elemento di $\widetilde{U}_s^0$ ed i coefficienti ξ_ν opportuni elementi di K. Si ha dunque

$$B(\boldsymbol{x},\ \boldsymbol{e}_{s+1}^*) = B(\boldsymbol{x}',\ \boldsymbol{e}_{s+1}) + \sum_{\nu \in (1,s)} \xi_\nu\, B(\boldsymbol{\epsilon}_\nu,\ \boldsymbol{e}_{s+1})$$

$$= \sum_{\nu \in (1,s)} \xi_\nu \left[B(\boldsymbol{e}_{s+1},\ \boldsymbol{\epsilon}_\nu) - \sum_{\mu \in (1,s)} B(\boldsymbol{\epsilon}_\mu,\ \boldsymbol{e}_{s+1})\, B(\boldsymbol{\epsilon}_\nu,\ \boldsymbol{e}_\mu) \right] = 0 ,$$

cioè risulterebbe dimostrata l'esistenza di un vettore $\boldsymbol{e}_{s+1}^*$ non nullo tale che

$$B(\boldsymbol{x},\ \boldsymbol{\epsilon}_{s+1}^*) = 0 \qquad \text{per } \forall \boldsymbol{x} \in V ,$$

ma ciò equivale a dire che V^0 contiene almeno un vettore non nullo, in contraddizione con l'ipotesi di B forma bilineare non degenere. La supposizione espressa

mediante la (5) non può dunque sussistere, quindi $\tilde{U}_s^0$ contiene almeno un vettore x^* tale che

$$B(e_{s+1}, x^*) = \xi \neq 0 . \tag{6}$$

Posto quindi $\epsilon_{s+1}^0 = x^*/\xi$ ed osservando che x^* appartiene ad U_s^0, che sussistono le (6) e (4), si ha che

$$B(\epsilon_{s+1}^0, e_\alpha) = \delta_{s+1,\alpha}, \qquad \alpha \in (1, s+1).$$

Posto ancora

$$\epsilon_\nu^0 = \epsilon_\nu - B(\epsilon_\nu, e_{s+1})\, \epsilon_{s+1}^0, \qquad \nu \in (1, s),$$

la famiglia $(\epsilon_\alpha^0)_{\alpha \in (1, s+1)}$ ovviamente soddisfa le

$$B(e_\alpha, \epsilon_\beta^0) = \delta_{\alpha\beta}, \qquad \alpha, \beta \in (1, s+1),$$

ed è libera.

La famiglia iniziale, costituita da s vettori, si può dunque ampliare in una avente $s+1$ vettori, e questo progressivo ampliamento cessa ovviamente quando la famiglia viene ad avere r elementi.

Si osservi ancora che lo spazio U^* sotteso dai vettori $(\epsilon_i)_{i \in (1,r)}$ non è univocamente determinato, potendosi ogni volta sostituire a ciascuno dei vettori ϵ_i ottenuti col procedimento costruttivo indicato sopra un vettore del tipo

$$\epsilon_i^* = \epsilon_i + u_i,$$

u_i essendo un qualsiasi elemento di U^0, senza con ciò ledere la validità delle (1).

Dal Teorema 1 si deduce infine il seguente

Corollario. *Se $U \subset V$ è non isotropo ed ha dimensione finita e se B è non degenere, $V = U \oplus U^0$.*

Questo corollario è conseguenza immediata del fatto che $U \cap U^0 = \{0\}$.

4. – Teorema 2. *Se $U \subset V$ ha dimensione finita ed è totalmente isotropo (o totalmente singolare) e B è non degenere, ad ogni base $(e_i)_{i \in (1,r)}$ di U si può far corrispondere una famiglia libera $(\epsilon_i)_{i \in (1,r)}$ di V tale che*

$$B(e_i, \epsilon_j) = \delta_{ij}, \qquad i, j \in (1, r),$$

e se $U^* = \bigoplus_{i \in (1,r)} K\epsilon_i$, che $U \oplus U^*$ sia non isotropo.

Dimostrazione. Anzitutto, dal Teorema 1 segue l'esistenza di una famiglia libera $(\epsilon_i)_{i\in(1,r)}$ dotata della proprietà indicata nell'enunciato, che inoltre genera lo spazio U^* e che è tale che

$$U^* \cap U^0 = \{0\}.$$

Essendo però U totalmente isotropo, $U \subset U^0$, quindi

$$U^* \cap U = \{0\},$$

ed è quindi lecito definire la somma diretta $U \oplus U^*$. Si ha ovviamente

$$\boldsymbol{x} = \sum_{i\in(1,r)} a_i \boldsymbol{e}_i + \sum_{i\in(1,r)} \alpha_i \boldsymbol{\epsilon}_i \qquad \text{per } \forall \boldsymbol{x} \in U \oplus U^*.$$

Se $U \oplus U^*$ fosse isotropo, $B(\boldsymbol{x}, \boldsymbol{x}) = 0$ implicherebbe

$$B(\boldsymbol{x}, \boldsymbol{e}_i) = 0, \quad B(\boldsymbol{x}, \boldsymbol{\epsilon}_i) = 0 \qquad \text{per } \forall i \in (1, r).$$

Ma U è totalmente isotropo, e quindi

$$B(\boldsymbol{e}_i, \boldsymbol{e}_j) = 0 \qquad \text{per } \forall i, j \in (1, r),$$

per cui la prima delle due condizioni indicate sopra diventa

$$B(\boldsymbol{x}, \boldsymbol{e}_i) = \alpha_i = 0 \qquad \text{per } \forall i \in (1, r),$$

cioè se sussiste l'isotropia di $U \oplus U^*$ il generico vettore appartenente a questo spazio deve anzitutto avere la forma $\boldsymbol{x} = \sum_{i\in(1,r)} y_i \boldsymbol{e}_i$. Perchè poi sia soddisfatta la seconda condizione dovrà essere

$$B(\boldsymbol{x}, \boldsymbol{\epsilon}_i) = a_i = 0 \qquad \text{per } \forall i \in (1, r)$$

e quindi $U \oplus U^* = \{0\}$. Ma se si esclude il caso banale di U vuoto, $U \oplus U^*$ non può ridursi a $\{0\}$ e quindi $U \oplus U^*$ è non isotropo, come appunto dovevasi dimostrare.

Teorema 3. *Se $U \subset V$ è totalmente isotropo (o totalmente singolare) ed ha dimensione finita, B è non degenere e J è uno spazio contenuto in V*

a) *totalmente isotropo (o rispettivamente totalmente singolare);*

b) *tale che* $J \cap U^0 = \{0\}$;

c) *tale che* $\dim_K J < \dim_K U$;

esiste uno spazio totalmente isotropo (o rispettivamente totalmente singolare) $U^* \subset V$ *tale che*

1) $J \subset U^*$;

2) $\dim_K U^* = \dim_K U$;

3) $U^* \cap U^0 = \{0\}$.

Dimostrazione. 1) Il teorema sarà dimostrato se si riesce ad ampliare J mantenendone la totale isotropia (rispettivamente totale singolarità): converrà dunque aggiungere ai vettori di una qualsiasi base di J un vettore z esterno a J: questo vettore z dovrà inoltre essere scelto in maniera che sia

$$(J \oplus Kz) \cap U^0 = \{0\},$$

poichè altrimenti i progressivi ampliamenti di J non condurrebbero ad uno spazio U^* dotato della proprietà espressa nel terzo comma della tesi. Deve dunque essere

$$z \notin (J \oplus U^0).$$

2) Si ha

$$J^0 \notin J \oplus U^0; \tag{1}$$

invero, se si suppone vero il contrario, cioè $J^0 \subseteq J \oplus U^0$, passando agli spazi ortogonali si trova $J \supseteq J^0 \cap U$ e quindi, tenuto conto dell'isotropia totale di U, $J \cap U^0 \supseteq J^0 \cap U$. Poichè, sempre per ipotesi, $J \cap U^0 = \{0\}$ sarebbe $J^0 \cap U = \{0\}$ e quindi $V \supseteq J^0 \oplus U$. Ma se fosse verificata la $J^0 \cap U = \{0\}$, per il Teorema 1 risulterebbe

$$\dim_K J = \dim_K (V \text{ modulo } J^0) \geqslant \dim_K U,$$

in contraddizione con l'ipotesi espressa mediante il comma c) dell'enunciato. Questa contraddizione dimostra dunque la (1).

3) Sussistendo la (1), basterà prendere $z \in J^0$ perchè siano verificate le

$$z \notin J, \quad z \perp J, \quad (J \oplus Kz) \cap U^0 = \{0\}. \tag{2}$$

Per completare la dimostrazione è necessario mostrare che si può scegliere z in modo che $J \oplus Kz$ sia totalmente isotropo (o totalmente singolare), cioè in modo che sia $B(z, z) = 0$ (o rispettivamente $Q(z) = 0$).

Si osservi anzitutto che aggiungendo al vettore z un vettore appartenente a $J^0 \cap (J \oplus U^0) = J \oplus J^0 \cap U^0$, oppure solamente a $J^0 \cap U^0$, le proprietà di z espresse mediante le (2) si mantengono invariate. Si aggiungerà dunque a z un elemento y appartenente allo spazio $J^0 \cap U^0$; anzi, si sceglierà y nello spazio $J^0 \cap U$, che è ovviamente un sottospazio di quello precedente che si è visto poc'anzi non essere vuoto. $z^* = z + y$ gode quindi di tutte le proprietà di z e deve inoltre essere

$$B(z^*, z^*) = B(z + y, z + y) = B(z, z) + 2\,B(z, y) = 0$$

(oppure, se U è totalmente singolare,

$$Q(z^*) = Q(z + y) = Q(z) + B(z, y) = 0)\,.$$

È sufficiente dimostrare che $z \notin (J^0 \cap U)^0$: infatti in tal caso esiste un $y_0 \in$ $\in J^0 \cap U$ tale che $B(z, y_0) = b$, $b \in K$, $b \neq 0$, ed un $k \in K$ tale che

$$B(z, z) + 2k\,b = 0$$

(oppure, se U è totalmente singolare,

$$Q(z) + k\,b = 0).$$

4) Per dimostrare che $z \notin (J^0 \cap U)^0$ basta osservare che

$$(J^0 \cap U)^0 \supseteq J \oplus U^0$$

e che si è proceduto alla scelta di z in modo che fosse $z \notin J \oplus U^0$: il risultato sarà acquisito se si mostra che $J \oplus U^0 = (J^0 \cap U)^0$. Ma l'ineguaglianza

$$\dim_K [V \text{ modulo } (J^0 \cap U)^0] \geqslant \dim_K [V \text{ modulo } (J^0 \oplus U)]$$

è equivalente alla relazione precedente. Inoltre il secondo membro di quest'ultima, essendo $J \cap U^0 = \{0\}$, vale $\dim_K U - \dim_K J$, mentre il primo membro è $\dim_K (J^0 \cap U)$. Si dovrà quindi verificare l'effettiva validità dell'ineguaglianza

$$\dim_K (J^0 \cap U) \geqslant \dim_K U - \dim_K J\,,$$

che si può riscrivere

$$\dim_K J \geqslant \dim_K U - \dim_K (J^0 \cap U)\,.$$

Ora questa a sua volta si riscrive

$$\dim_K (V \text{ modulo } J^0) \geqslant \dim_K [U \text{ modulo } (J^0 \cap U)]$$

ed in questa ultima forma risulta evidente, per cui il Teorema 3 è dimostrato.

Dal Teorema 3 si deduce il seguente

Corollario. *Se U è uno spazio totalmente isotropo (o totalmente singolare) di dimensione massima e finita contenuto in V, tutti gli altri spazi totalmente isotropi (o totalmente singolari) di dimensione massima contenuti in V hanno la dimensione di U.*

Dimostrazione. Sia U un sottospazio totalmente isotropo (o totalmente singolare) di dimensione finita e massimale. Allora si potrà scrivere $\dim_K U = r < \infty$, ed evidentemente lo spazio U non si potrà ulteriormente ampliare in uno spazio totalmente isotropo (o, rispettivamente, totalmente singolare).

Per quanto è stato dimostrato col Teorema 3, si potrà scegliere in V uno spazio totalmente isotropo (rispettivamente, totalmente singolare) tale che

$$\dim_K J = r, \qquad J \cap U^0 = \{0\}$$

e quindi $J \oplus U$ è non isotropo. Segue da ciò che

$$V = U \oplus J \oplus (U \oplus J)^0.$$

Si supponga ora che possa esistere in V un altro spazio U^* totalmente isotropo (o totalmente singolare) non ulteriormente ampliabile sotto l'ipotesi di conservazione di questa proprietà, diverso da U e di dimensione superiore ad r. Poichè $\dim_K J = r$, $U^* \cap [U \oplus (U \oplus J)^0] \neq \{0\}$. Di conseguenza $\forall x \in U^* \cap \cap [u \oplus (u \oplus J)^0]$ è tale che

$$x = x_1 + x_2 \qquad \text{con} \quad x_1 \in U, \; x_2 \in (U \oplus J)^0.$$

Ma essendo $x_2 \perp U$, $B(x_1, x_2) = 0$ per cui

$$B(x, x) = 0 \implies B(x_2, x_2) = 0$$

(oppure

$$Q(x) = 0 \implies Q(x_2) = 0).$$

U essendo uno spazio totalmente isotropo (o totalmente singolare) di dimensione massimale, necessariamente x_2 è nullo, cioè $x \in U \cap U^*$. Si consideri ora un vettore y di J che si dirà corrispondente ad $x \in U$ se $B(x, y) = 1$. Ovviamente lo spazio $\{x, y\}$ generato da x ed y non è isotropo e quindi

$$V = \{x, y\} \oplus \{x, y\}^0 ,$$

per cui si potrà scrivere

$$U = \{x\} \oplus [U \cap \{x, y\}^0] , \qquad U^* = \{x\} \oplus [U^* \cap \{x, y\}^0] .$$

Orbene, si verifica immediatamente che la restrizione della forma quadratica Q ad $\{x, y\}^0$ è non degenere, che $U \cap \{x, y\}^0$ ed $U^* \cap \{x, y\}^0$ sono sottospazi totalmente isotropi (rispettivamente, totalmente singolari) massimali in $\{x, y\}^0$ e che

$$\dim_K [U \cap \{x, y\}^0] = \dim_K U - 1, \qquad \dim_K [U^* \cap \{x, y\}^0] = \dim_K U^* - 1 .$$

La dimostrazione del teorema è quindi ricondotta dal caso di $\dim_K U$ al caso di $\dim_K U - 1$ e quindi, ripetendo il procedimento un numero sufficiente e finito di volte, si è portati a considerare il teorema per il caso di $\dim_K U = 0$: in questo caso però ovviamente $\dim_K U = \dim_K U^*$ e con ciò si conclude la dimostrazione.

5. – Per completare questi risultati si osservi che se il campo K ha caratteristica 2 ogni elemento dello spazio V è isotropo e quindi nella decomposizione

$$V = U \oplus J \oplus (U \oplus J)^0$$

di V, lo spazio non isotropo $(U \oplus J)^0$ è necessariamente vuoto per cui $V = U \oplus J$, cioè se K ha caratteristica 2

$$\dim_K V = 2 \dim_K U .$$

Un'altra conseguenza del Teorema 3 e del suo corollario è che se V ha dimensione finita la dimensione degli spazi totalmente isotropi (o totalmente singolari) contenuti in V non supera mai l'intero $[(\dim_K V)/2]$. Se K è quadraticamente chiuso, la dimensione degli spazi totalmente singolari contenuti in V raggiunge effettivamente questo valore.

Alla decomposizione

$$V = U \oplus J \oplus (U \oplus J)^0 = U \oplus J \oplus C$$

di V in due spazi totalmente isotropi (o totalmente singolari) disgiunti U e J di eguale dimensione ed in uno spazio non isotropo C ortogonale alla loro somma diretta si dà il nome di *decomposizione di Witt* dello spazio V: alle due basi di U e J scelte in maniera da soddisfare le condizioni dell'enunciato del Teorema 2 si darà nel seguito il nome di basi *concatenate*.

6. - Il gruppo ortogonale.

Ogni applicazione lineare $\boldsymbol{x} \to \mathscr{L}\boldsymbol{x}$ dello spazio vettoriale V in sè stesso, tale che

$$Q(\mathscr{L}\boldsymbol{x}) = Q(\boldsymbol{x}) , \tag{1}$$

si chiama *trasformazione ortogonale* di V. Se B denota la forma bilineare associata a Q, segue immediatamente dalle definizioni che

$$B(\mathscr{L}\boldsymbol{x},\ \mathscr{L}\boldsymbol{y}) = B(\boldsymbol{x},\ \boldsymbol{y}), \tag{2}$$

Inoltre, se

$$\operatorname{Ker} \mathscr{L} = \{ \boldsymbol{x} \in V \mid \mathscr{L}\boldsymbol{x} = 0 \},$$

si ha

$$\operatorname{Ker} \mathscr{L} = \{ 0 \}.$$

Le trasformazioni ortogonali di V sono dunque automorfismi di questo spazio vettoriale: la totalità di queste trasformazioni costituisce un gruppo, che si chiama *gruppo ortogonale di* Q, e si segna $G = O(Q)$.

Le condizioni, fra di loro equivalenti, (1) e (2) permettono di affermare immediatamente che qualsiasi elemento del gruppo G conserva

a) l'ortogonalità di due elementi di V;
b) l'isotropia di un elemento di V;
c) la singolarità di un elemento di V.

Di conseguenza spazi coniugati, spazi isotropi, spazi totalmente isotropi o spazi totalmente singolari sono trasformati da elementi del gruppo ortogonale sempre in spazi coniugati, spazi isotropi, spazi totalmente isotropi o spazi totalmente singolari.

7. - Le simmetrie.

Siano V uno spazio vettoriale di dimensione finita definito su un campo K, Q una forma quadratica non degenere definita su V e B la forma bilineare associata a Q.

Si consideri un iperpiano $H \subset V$ tale che il suo spazio coniugato H^0 contenga *almeno un* vettore non singolare $\boldsymbol{h}$, e l'applicazione lineare $\boldsymbol{x} \to \mathscr{S}_h \boldsymbol{x}$ di V in V definita mediante la formula

$$\mathscr{S}_h \boldsymbol{x} = \boldsymbol{x} - Q^{-1}(\boldsymbol{h})\, B(\boldsymbol{h},\ \boldsymbol{x})\, \boldsymbol{h} \qquad \text{per } \forall\, \boldsymbol{x} \in V\,.$$

L'applicazione $\mathscr{S}_h$ gode delle seguenti proprietà:

1) *$\mathscr{S}_h$ è una trasformazione ortogonale.*

Infatti

$$Q(\mathscr{S}_h \boldsymbol{x}) = Q(\boldsymbol{x} - Q^{-1}(\boldsymbol{h})\, B(\boldsymbol{h},\ \boldsymbol{x})\, \boldsymbol{h}) =$$

$$= Q(\boldsymbol{x}) + Q^{-2}(\boldsymbol{h})\, B^2(\boldsymbol{h},\ \boldsymbol{x})\, Q(\boldsymbol{h}) - Q^{-1}(\boldsymbol{h})\ B^2(\boldsymbol{h},\ \boldsymbol{x}) = Q(\boldsymbol{x})\,.$$

2) *$\mathscr{S}_h$ lascia fissi tutti gli elementi di H.*

Infatti

$$B(\boldsymbol{h},\ \boldsymbol{x}) = 0 \qquad \text{per } \forall \boldsymbol{x} \in H,$$

quindi

$$\mathscr{S}_h \boldsymbol{x} = \boldsymbol{x} \qquad \text{per } \forall \boldsymbol{x} \in H\,.$$

3) *$\mathscr{S}_h$ trasforma ogni elemento non singolare di H^0 nel suo opposto.*

Infatti ogni elemento non singolare di H^0 può scriversi

$$\boldsymbol{x} = k\,\boldsymbol{h} \qquad \text{con } k \in K,\ k \neq 0,$$

per cui

$$\mathscr{S}_h\,(k\,\boldsymbol{h}) = k\,\boldsymbol{h} - Q^{-1}(\boldsymbol{h})\, B(k\,\boldsymbol{h},\ \boldsymbol{h})\boldsymbol{h} = k\,\boldsymbol{h} - Q^{-1}(\boldsymbol{h})\, k\, B(\boldsymbol{h},\ \boldsymbol{h})\, \boldsymbol{h}$$

$$= k\,\boldsymbol{h} - 2k\, Q^{-1}(\boldsymbol{h})\, Q(\boldsymbol{h})\, \boldsymbol{h} = -\,k\,\boldsymbol{h}\,.$$

4) *Esclusa la trasformazione identica, $\mathscr{S}_h$ è il solo elemento del gruppo G che lascia fissi tutti gli elementi di H.*

Sia $\mathscr{L}^*$ un elemento di G avente la proprietà indicata nell'enunciato: allora per $\forall \boldsymbol{x} \in H^0$ si ha

$$\mathscr{L}^* \boldsymbol{x} \neq \boldsymbol{x} ,$$

perchè altrimenti aggiungendo ad una qualsiasi base di H uno di questi elementi di H^0 lasciati fissi dalla $\mathscr{L}^*$, si otterrebbe una base di V di cui ogni elemento rimarrebbe fisso per $\mathscr{L}^*$, sicchè $\mathscr{L}^*$ lascerebbe fisso ogni vettore di V, cioè si ridurrebbe alla trasformazione identica, che è però stata esclusa per ipotesi. Dunque

$$\boldsymbol{\xi} = \mathscr{L}^* \boldsymbol{x} - \boldsymbol{x} \neq 0 ,$$

ed il vettore così definito sicuramente appartiene ad $H^0 = K\,\boldsymbol{h}$, perchè detto $\boldsymbol{y}$ un qualsiasi vettore di H,

$$B(\boldsymbol{\xi}, \boldsymbol{y}) = B(\mathscr{L}^*\boldsymbol{x}, \boldsymbol{y}) - B(\boldsymbol{x}, \boldsymbol{y}) = B(\mathscr{L}^*\boldsymbol{x}, \mathscr{L}^*\boldsymbol{y}) - B(\boldsymbol{x}, \boldsymbol{y}) = B(\boldsymbol{x}, \boldsymbol{y}) - B(\boldsymbol{x}, \boldsymbol{y}) = 0.$$

Quindi $\boldsymbol{\xi} \in H^0$, cioè $\boldsymbol{\xi} = k\,\boldsymbol{h}$, $k \in K$, $k \neq 0$. Conseguentemente

$$\mathscr{L}^*\boldsymbol{x} = \boldsymbol{x} + k\,\boldsymbol{h} .$$

Ma poichè $\mathscr{L}^*$ è una trasformazione ortogonale, deve essere

$$Q(\mathscr{L}^*\boldsymbol{x}) = Q(\boldsymbol{x}),$$

cioè

$$Q(\boldsymbol{x}) + k^2\, Q(\boldsymbol{h}) + k\, B(\boldsymbol{h}, \boldsymbol{x}) = Q(\boldsymbol{x}),$$

ossia

$$k[k\, Q(\boldsymbol{h}) + B(\boldsymbol{h}, \boldsymbol{x})] = 0 .$$

La soluzione $k = 0$ di quest'equazione è da escludersi per quanto si è visto poc'anzi e quindi

$$k = -\, Q^{-1}(\boldsymbol{h})\, B(\boldsymbol{h}, \boldsymbol{x}) ,$$

per cui

$$\mathscr{L}^* \boldsymbol{x} = \boldsymbol{x} - Q^{-1}(\boldsymbol{h})\, B(\boldsymbol{h},\ \boldsymbol{x})\, \boldsymbol{h} = \mathscr{S}_h \boldsymbol{x}\,.$$

5) *Se* $k \in K,\ k \neq 0,\ 1,\ \mathscr{S}_h = \mathscr{S}_{kh}$.

Infatti

$$\mathscr{S}_{kh}\boldsymbol{x} = \boldsymbol{x} - Q^{-1}(k\,\boldsymbol{h})\, B(k\,\boldsymbol{h},\ \boldsymbol{x})\, k\,\boldsymbol{h} = \boldsymbol{x} - k^{-2}\, Q^{-1}(\boldsymbol{h})\, k\, B(\boldsymbol{h},\ \boldsymbol{x})\, k\,\boldsymbol{h}$$
$$= \boldsymbol{x} - Q^{-1}(\boldsymbol{h})\, B(\boldsymbol{h},\ \boldsymbol{x})\, \boldsymbol{h} = \mathscr{S}_h \boldsymbol{x}\,.$$

6) $\mathscr{S}_h$ *è una trasformazione involutiva.*

Infatti

$$\mathscr{S}_h(\mathscr{S}_h \boldsymbol{x}) = \mathscr{S}_h[\boldsymbol{x} - Q^{-1}(\boldsymbol{h})\, B(\boldsymbol{h},\ \boldsymbol{x})\, \boldsymbol{h}] =$$
$$= \boldsymbol{x} - Q^{-1}(\boldsymbol{h})\, B(\boldsymbol{h},\ \boldsymbol{x})\, \boldsymbol{h} - Q^{-1}(\boldsymbol{h})\, B[\boldsymbol{x} - Q^{-1}(\boldsymbol{h})\, B(\boldsymbol{h},\ \boldsymbol{x})\, \boldsymbol{h},\ \boldsymbol{h}]\, \boldsymbol{h}$$
$$= \boldsymbol{x} - Q^{-1}(\boldsymbol{h})\, B(\boldsymbol{h},\ \boldsymbol{x})\, \boldsymbol{h} - Q^{-1}(\boldsymbol{h})\, B(\boldsymbol{h},\ \boldsymbol{x})\, \boldsymbol{h} + Q^{-2}(\boldsymbol{h})\, B(\boldsymbol{h},\ \boldsymbol{x}) B(\boldsymbol{h},\ \boldsymbol{h})\, \boldsymbol{h}$$
$$= \boldsymbol{x} - 2\, Q^{-1}(\boldsymbol{h})\, B(\boldsymbol{h},\ \boldsymbol{x})\, \boldsymbol{h} + 2\, Q^{-1}(\boldsymbol{h})\, B(\boldsymbol{h},\ \boldsymbol{x})\, \boldsymbol{h} = \boldsymbol{x}\,,$$

cioè

$$\mathscr{S}_h \mathscr{S}_h = \mathscr{I}\,.$$

L'applicazione $\mathscr{S}_h$ dipende unicamente dalla scelta di H e viene perciò chiamata *simmetria rispetto all'iperpiano* H che, per l'ipotesi iniziale, si supporrà sempre dotato di vettori ortogonali non singolari. La totalità delle simmetrie genera un gruppo, che verrà nel seguito indicato come G' e per il quale si può ovviamente scrivere $G' \subseteq G$.

8. – Lemma A. *Se*

$$1)\quad \boldsymbol{a},\ \boldsymbol{b} \in V \mid Q(\boldsymbol{a}) = Q(\boldsymbol{b})\,,$$
$$2)\quad \boldsymbol{n} = \boldsymbol{a} - \boldsymbol{b} \mid Q(\boldsymbol{n}) \neq 0\,,$$

si ha

$$\mathscr{S}_n \boldsymbol{b} = \boldsymbol{a}\,.$$

La dimostrazione di questo lemma è una conseguenza immediata delle definizioni: si ha infatti

$$\mathscr{S}_n \boldsymbol{b} = \boldsymbol{b} - Q^{-1}(\boldsymbol{n})\, B(\boldsymbol{n}, \boldsymbol{b})\, \boldsymbol{n} = \boldsymbol{b} - Q^{-1}(\boldsymbol{n})[Q(\boldsymbol{n} + \boldsymbol{b}) - Q(\boldsymbol{n}) - Q(\boldsymbol{b})]\boldsymbol{n}$$

$$= \boldsymbol{b} - Q^{-1}(\boldsymbol{n})[Q(\boldsymbol{a}) - Q(\boldsymbol{n}) - Q(\boldsymbol{a})]\boldsymbol{n} = \boldsymbol{b} + \boldsymbol{n} = \boldsymbol{a}\,.$$

Lemma B. *Se* $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{a}^*, \boldsymbol{b}^*$ *sono elementi di* V *tali che*

$$Q(\boldsymbol{a}) = Q(\boldsymbol{b}) = Q(\boldsymbol{a}^*) = Q(\boldsymbol{b}^*) = 0, \qquad B(\boldsymbol{a}, \boldsymbol{a}^*) = B(\boldsymbol{b}, \boldsymbol{b}^*) = 1,$$

esiste un elemento $\mathscr{S}$ *di* G' *tale che*

$$\mathscr{S}\boldsymbol{b} = \boldsymbol{a}\,.$$

Nel dimostrare questo lemma conviene distinguere due casi:

a) Uno dei due vettori

$$\boldsymbol{d} = \boldsymbol{a} - \boldsymbol{b}, \qquad \boldsymbol{d}^* = \boldsymbol{a}^* - \boldsymbol{b}^*,$$

ad esempio $\boldsymbol{d}$, è non singolare. Si può allora applicare immediatamente il Lemma A e quindi, essendo

$$\mathscr{S}_d \boldsymbol{b} = \boldsymbol{a},$$

$\mathscr{S}_d$ è l'elemento $\mathscr{S}$ cercato. Se invece $\boldsymbol{d}^*$ è non singolare, basterà scambiare fra di loro i vettori asteriscati ed i vettori non asteriscati, che comunque occupano nell'enunciato una posizione perfettamente simmetrica.

b) Ambedue i vettori $\boldsymbol{d}, \boldsymbol{d}^*$ sono singolari. Allora da

$$Q(\boldsymbol{d}^*) = Q(\boldsymbol{a}^* - \boldsymbol{b}^*) = Q(\boldsymbol{a}^*) + Q(\boldsymbol{b}^*) - B(\boldsymbol{a}^*, \boldsymbol{b}^*) = 0$$

segue che

$$B(\boldsymbol{a}^*, \boldsymbol{b}^*) = 0\,,$$

per cui ciascun vettore della forma

$$\boldsymbol{u}^* = p\,\boldsymbol{a}^* + q\,\boldsymbol{b}^*, \qquad \text{per } \forall p,\ q \in K$$

è singolare. Posto allora

$$\boldsymbol{n}_1 = \boldsymbol{b} - \boldsymbol{u}^*, \qquad \boldsymbol{n}_2 = \boldsymbol{u}^* - \boldsymbol{a},$$

si ha invece

$$\begin{aligned} Q(\boldsymbol{n}_1) = Q(\boldsymbol{b} - \boldsymbol{u}^*) &= Q(\boldsymbol{b}) + Q(\boldsymbol{u}^*) - B(\boldsymbol{b}, \boldsymbol{u}^*) = -B(\boldsymbol{b}, p\,\boldsymbol{a}^* + q\,\boldsymbol{b}^*) \\ &= -q - p\,B(\boldsymbol{b}, \boldsymbol{a}^*), \end{aligned}$$

$$\begin{aligned} Q(\boldsymbol{n}_2) = Q(\boldsymbol{u}^* - \boldsymbol{a}) &= Q(\boldsymbol{u}^*) + Q(\boldsymbol{a}) - B(\boldsymbol{a}, \boldsymbol{u}^*) = -B(\boldsymbol{a}, p\,\boldsymbol{a}^* + q\,\boldsymbol{b}^*) \\ &= -p - q\,B(\boldsymbol{a}, \boldsymbol{b}^*), \end{aligned}$$

ed è sempre possibile scegliere p e q in K in modo che sia

$$Q(\boldsymbol{n}_1) \neq 0, \qquad Q(\boldsymbol{n}_2) \neq 0,$$

cioè che i vettori $\boldsymbol{n}_1$ ed $\boldsymbol{n}_2$ siano non singolari.

Per il Lemma A, essendo $\boldsymbol{n}_1 = \boldsymbol{b} - \boldsymbol{u}^*$,

$$\mathcal{S}_{n_1}\boldsymbol{b} = \boldsymbol{u}^*,$$

e, sempre per il medesimo lemma, essendo $\boldsymbol{n}_2 = \boldsymbol{u}^* - \boldsymbol{a}$,

$$\mathcal{S}_{n_2}\mathcal{S}_{n_1}\boldsymbol{b} = \mathcal{S}_{n_2}\boldsymbol{u}^* = \boldsymbol{a},$$

sicchè

$$\mathcal{S}_{n_2}\mathcal{S}_{n_1} = \mathcal{S}$$

è l'elemento di G' cercato.

Parte prima

9. - Il Teorema di Cartan e Dieudonné. Prima dimostrazione.

Sia V uno spazio vettoriale di dimensione finita, definito sul campo K e dotato di forma quadratica non degenere Q. Allora, escludendo il caso di $K = GF(2)$, $\dim_K V = 4$, $\dim_K S = 2$, ove S è un sottospazio totalmente singolare di dimensione massima in V, si ha

$$G' = G.$$

Dimostrazione.

1) Sia S uno qualsivoglia degli spazi totalmente singolari massimali di V: allora, per la decomposizione di WITT, esiste un secondo spazio totalmente singolare massimale R in V, tale che

$$S \cap R = \{0\}, \qquad V = S \oplus R \oplus (S \oplus R)^0 .$$

Sempre per la decomposizione di WITT si è visto che S ha una base $(e_i)_{i\in(1,r)}$ ed R ha una base $(\epsilon_j)_{j\in(1,r)}$ tali che

$$B(e_i, \epsilon_j) = \delta_{ij}, \qquad i, j \in (1, r), \tag{1}$$

r essendo la dimensione di S e B la forma bilineare associata a Q. Sia $\mathcal{T}$ un qualsiasi elemento del gruppo G e si considerino gli elementi $\mathcal{S}$ del gruppo G': allora, ad ogni coppia $\mathcal{T}$, $\mathcal{S}$ si potrà far corrispondere un intero

$$0 \leqslant m_S(\mathcal{T}, \mathcal{S}) \leqslant r,$$

tale che per $i \leqslant m_S(\mathcal{T}, \mathcal{S})$ sia

$$\mathcal{S}e_i = \mathcal{T}e_i, \qquad \mathcal{S}\epsilon_i = \mathcal{T}\epsilon_i,$$

mentre per $i = m_S(\mathcal{T}, \mathcal{S}) + 1$ *almeno* una delle

$$\mathcal{S}e_i = \mathcal{T}e_i, \qquad \mathcal{S}\epsilon_i = \mathcal{T}\epsilon_i,$$

non sia verificata.

Scelto ora un determinato elemento $\mathcal{T}$ del gruppo G, si considerino i vari elementi $\mathcal{S}$ del gruppo G' ed i corrispondenti interi $m_S(\mathcal{T}, \mathcal{S})$ e si indichi con m il valore massimo raggiunto da questi interi. Giova qui osservare ancora che scelto $\mathcal{T}$, l'intero $m_S(\mathcal{T}, \mathcal{S})$ varia anche in funzione di S: si supporrà quindi nel seguito che sia stato scelto quale spazio S in V quello spazio totalmente singolare massimale che permette di raggiungere il più alto possibile valore di m.

2) La dimostrazione del teorema procede in due tappe essenziali. Nella prima di esse si vedrà che, escludendo il caso specificato nell'enunciato del teorema, si ha sempre $m = r$.

Sia dunque $\mathcal{S}$ uno degli elementi del gruppo G' per i quali $m_S(\mathcal{T}, \mathcal{S})$ raggiunge effettivamente il suo valore massimo m e si ponga

$$S_m = \bigoplus_{i\in(1,r)} Ke_i, \qquad R_m = \bigoplus_{i\in(1,r)} K\epsilon_i .$$

Gli spazi S_m ed R_m sono totalmente singolari e, per la definizione dell'intero m,

$$\mathscr{S}\boldsymbol{x} = \mathscr{T}\boldsymbol{x} \qquad \text{per } \forall\, \boldsymbol{x} \in S_m \oplus R_m .$$

Inoltre, sempre per le definizioni e nel caso che si supponga $m < r$, *almeno una* delle due relazioni

$$\mathscr{S}\boldsymbol{e}_{m+1} = \mathscr{T}\boldsymbol{e}_{m+1}, \qquad \mathscr{S}\boldsymbol{\epsilon}_{m+1} = \mathscr{T}\boldsymbol{\epsilon}_{m+1}$$

è sicuramente falsa.

Orbene, si mostrerà anzitutto che è sempre lecito supporre vera una di queste equazioni, ad esempio la

$$\mathscr{S}\boldsymbol{e}_{m+1} = \mathscr{T}\boldsymbol{e}_{m+1} .$$

Infatti $\mathscr{S}$ e $\mathscr{T}$ sono ambedue trasformazioni ortogonali e sussistono le (1), quindi lo spazio

$$\mathscr{S}S_m \oplus \mathscr{S}R_m = \mathscr{T}S_m \oplus \mathscr{T}R_m$$

è ortogonale ai vettori

$$\mathscr{S}\boldsymbol{e}_{m+1}, \quad \mathscr{T}\boldsymbol{e}_{m+1}, \quad \mathscr{S}\boldsymbol{\epsilon}_{m+1}, \quad \mathscr{T}\boldsymbol{\epsilon}_{m+1}$$

e quindi le simmetrie definite mediante vettori *non singolari* contenuti nello spazio

$$V_4 = K\mathscr{S}\boldsymbol{e}_{m+1} \oplus K\mathscr{T}\boldsymbol{e}_{m+1} \oplus K\mathscr{S}\boldsymbol{\epsilon}_{m+1} \oplus K\mathscr{T}\boldsymbol{\epsilon}_{m+1}$$

lasciano fissi tutti i vettori degli spazi $\mathscr{S}S_m$ e $\mathscr{T}R_m$.

Si può pertanto applicare a V_4 il Lemma B, quindi esiste un elemento $\mathscr{S}_4$ del gruppo G_4' delle simmetrie in V_4 tale che

$$\mathscr{S}_4\mathscr{S}\boldsymbol{e}_{m+1} = \mathscr{T}\boldsymbol{e}_{m+1} .$$

$\mathscr{S}_4$ è il prodotto di simmetrie rispetto a vettori contenuti in V_4 quindi l'estensione $\mathscr{S}^*$ di $\mathscr{S}_4$ a tutto V sarà il prodotto di simmetrie in V rispetto a vettori di $V_4 \subset V$, cioè $\mathscr{S}^*$ sarà un elemento di G', il quale, per quanto si è visto, sarà tale che

$$\mathscr{S}^*\mathscr{S}\boldsymbol{e}_{m+1} = \mathscr{T}\boldsymbol{e}_{m+1},$$

$$\mathscr{S}^*\mathscr{S}\boldsymbol{e}_i = \mathscr{T}\boldsymbol{e}_i, \quad \mathscr{S}^*\mathscr{S}\boldsymbol{\epsilon}_i = \mathscr{T}\boldsymbol{\epsilon}_i, \qquad i \in (1,\ m) .$$

È dunque lecito supporre che si sia proceduto sin dal principio alla scelta di un elemento di G' per il quale sia $m_s(\mathcal{T}, \mathcal{S}) = m$ e

$$\mathcal{S}\boldsymbol{e}_{m+1} = \mathcal{T}\boldsymbol{e}_{m+1} .$$

3) Segue immediatamente da quest'ultimo risultato che il vettore

$$\boldsymbol{\sigma} = \mathcal{T}\boldsymbol{\epsilon}_{m+1} - \mathcal{S}\boldsymbol{\epsilon}_{m+1}$$

è singolare. Se ciò non fosse, $\boldsymbol{\sigma}$ permetterebbe di definire una simmetria $\mathcal{S}_\sigma$ e, assieme alle

$$\mathcal{S}_\sigma \mathcal{S}\boldsymbol{e}_i = \mathcal{T}\boldsymbol{e}_i, \qquad \mathcal{S}_\sigma \mathcal{S}\boldsymbol{\epsilon}_i = \mathcal{T}\boldsymbol{\epsilon}_i, \qquad i \in (1,\ m) ,$$

essendo ancora

$$B(\mathcal{S}\boldsymbol{e}_{m+1},\ \boldsymbol{\sigma}) = B(\mathcal{S}\boldsymbol{e}_{m+1},\ \mathcal{T}\boldsymbol{\epsilon}_{m+1}) - B(\mathcal{S}\boldsymbol{e}_{m+1},\ \mathcal{S}\boldsymbol{\epsilon}_{m+1}) =$$

$$= B(\mathcal{T}\boldsymbol{e}_{m+1},\ \mathcal{T}\boldsymbol{\epsilon}_{m+1}) - 1 = 0 , \tag{2}$$

sarebbe

$$\mathcal{S}_\sigma \mathcal{S}\boldsymbol{e}_{m+1} = \mathcal{S}\boldsymbol{e}_{m+1} = \mathcal{T}\boldsymbol{e}_{m+1},$$

ed infine, per il Lemma A,

$$\mathcal{S}_\sigma\ \mathcal{S}\boldsymbol{\epsilon}_{m+1} = \mathcal{T}\boldsymbol{\epsilon}_{m+1},$$

per cui m cesserebbe di essere il valore massimo raggiungibile da $m_s(\mathcal{T}, \mathcal{S})$ al variare di $\mathcal{S}$ in G', contrariamente all'ipotesi. $\boldsymbol{\sigma}$ è quindi necessariamente singolare.

Conseguentemente, dalla

$$Q(\mathcal{T}\boldsymbol{\epsilon}_{m+1}) = Q(\boldsymbol{\sigma} + \mathcal{S}\boldsymbol{\epsilon}_{m+1}) = Q(\boldsymbol{\sigma}) + Q(\mathcal{S}\boldsymbol{\epsilon}_{m+1}) + B(\boldsymbol{\sigma},\ \mathcal{S}\boldsymbol{\epsilon}_{m+1}) = 0$$

segue che

$$B(\mathcal{S}\boldsymbol{\epsilon}_{m+1},\ \boldsymbol{\sigma}) = 0 . \tag{3}$$

Dalla (2) e dalla (3) risulta che

$$\boldsymbol{\sigma} \notin K\mathcal{S}\boldsymbol{e}_{m+1},$$

per cui lo spazio $K\mathscr{S}\boldsymbol{e}_{m+1} \oplus K\boldsymbol{\sigma}$ risulta essere: a) totalmente singolare, per via della (2); b) ortogonale allo spazio $\mathscr{S}S_m \oplus \mathscr{S}R_m$, per via della (1).

Quindi

$$(\mathscr{S}S_m \oplus \mathscr{S}R_m)^0 \supset K\mathscr{S}\boldsymbol{e}_{m+1} \oplus K\boldsymbol{\sigma}\,,$$

e lo spazio al primo membro essendo coniugato ad uno spazio non singolare è a sua volta non singolare: contiene però uno spazio totalmente singolare di dimensione 2 e quindi per la decomposizione di WITT necessariamente contiene un secondo spazio totalmente singolare di dimensione che col primo ha in comune solamente il vettore nullo. Poichè

$$\dim_K(\mathscr{S}S_m \oplus \mathscr{S}R_m) = n - 2m,$$

dovrà essere $n - 2m \geqslant 4$ cioè $n \geqslant 2m + 4$.

4) Si vede immediatamente che l'ipotesi

$$\dim_K V = n > 2m + 4$$

conduce ad una contraddizione con l'ipotesi di massimalità di m. Invero, $\mathscr{S}\boldsymbol{\epsilon}_{m+1}$ è contenuto in $(\mathscr{S}S_m \oplus \mathscr{S}R_m)^0$, come subito si vede facendo uso della (1), e quindi quale secondo spazio totalmente singolare contenuto in $(\mathscr{S}S_m \oplus \mathscr{S}R_m)^0$ si potrà considerare lo spazio sotteso dai vettori $\mathscr{S}\boldsymbol{\epsilon}_{m+1}$ e $\boldsymbol{\sigma}^*$: l'esistenza di un vettore $\boldsymbol{\sigma}^*$, singolare e soddisfacente alle

$$B(\mathscr{S}\boldsymbol{e}_{m+1},\ \boldsymbol{\sigma}^*) = B(\mathscr{S}\boldsymbol{\epsilon}_{m+1},\ \boldsymbol{\sigma}^*) = 0, \qquad B(\boldsymbol{\sigma},\ \boldsymbol{\sigma}^*) = 1\,,$$

è assicurata dal procedimento costruttivo fornito nella dimostrazione relativa alla decomposizione di WITT. Estendendo la definizione di S_m ed R_m, si potrà scrivere ancora

$$\mathscr{S}S_{m+1} \oplus K\boldsymbol{\sigma} \oplus \mathscr{S}R_{m+1} \oplus K\boldsymbol{\sigma}^* \supset \mathscr{S}S_m \oplus \mathscr{S}R_m,$$

cioè

$$(\mathscr{S}S_m \oplus \mathscr{S}R_m)^0 \supset (\mathscr{S}S_{m+1} \oplus K\boldsymbol{\sigma} \oplus \mathscr{S}R_{m+1} \oplus K\boldsymbol{\sigma}^*)^0.$$

Se $n > 2m + 4$, cioè se $n - 2m > 4$, per quanto è stato dimostrato in relazione alla decomposizione di WITT, esiste in $(\mathscr{S}S_m \oplus \mathscr{S}R_m)^0$ un vettore $\boldsymbol{n}$ non singolare.

Si considerino allora i vettori

$$\boldsymbol{s} = \mathcal{S}\boldsymbol{\epsilon}_{m+1} + \boldsymbol{u} - Q(\boldsymbol{u})\,\mathcal{S}\boldsymbol{e}_{m+1},$$

$$\boldsymbol{n}_1 = \boldsymbol{s} - \mathcal{S}\boldsymbol{\epsilon}_{m+1} = \boldsymbol{u} - Q(\boldsymbol{u})\,\mathcal{S}\boldsymbol{e}_{m+1},$$

$$\boldsymbol{n}_2 = \boldsymbol{\sigma} - \boldsymbol{n}_1 = \boldsymbol{\sigma} - \boldsymbol{s} + \mathcal{S}\boldsymbol{\epsilon}_{m+1} = \boldsymbol{\sigma} - \boldsymbol{u} + Q(\boldsymbol{u})\,\mathcal{S}\boldsymbol{e}_{m+1}.$$

Si ha:

$$Q(\boldsymbol{s}) = Q(\mathcal{S}\boldsymbol{\epsilon}_{m+1}) + Q(\boldsymbol{u}) + Q^2(\boldsymbol{u})\,Q(\mathcal{S}\boldsymbol{e}_{m+1}) + B(\mathcal{S}\boldsymbol{\epsilon}_{m+1},\ \boldsymbol{u}) - Q(\boldsymbol{u})\,B(\mathcal{S}\boldsymbol{\epsilon}_{m+1}, \mathcal{S}\boldsymbol{e}_{m+1})$$

$$- Q(\boldsymbol{u})\,B(\boldsymbol{u},\ \mathcal{S}\boldsymbol{e}_{m+1}) = Q(\boldsymbol{u}) - Q(\boldsymbol{u})\,B(\boldsymbol{\epsilon}_{m+1},\ \boldsymbol{e}_{m+1}) = 0\,,$$

$$Q(\boldsymbol{n}_1) = Q(\boldsymbol{u}) + Q^2(\boldsymbol{u})\,Q(\mathcal{S}\boldsymbol{e}_{m+1}) - Q(\boldsymbol{u})\,B(\boldsymbol{u},\ \mathcal{S}\boldsymbol{e}_{m+1}) = Q(\boldsymbol{u}) \neq 0\,,$$

$$Q(\boldsymbol{n}_2) = Q(\boldsymbol{\sigma}) + Q(\boldsymbol{n}_1) - B(\boldsymbol{\sigma},\ \boldsymbol{n}_1) = Q(\boldsymbol{n}_1) = Q(\boldsymbol{u}) \neq 0\,.$$

Applicando quindi il Lemma A, si ha

$$\mathcal{S}_{\boldsymbol{n}_1}\mathcal{S}\boldsymbol{\epsilon}_{m+1} = \boldsymbol{s}, \qquad \mathcal{S}_{\boldsymbol{n}_2}\mathcal{S}_{\boldsymbol{n}_1}\mathcal{S}\boldsymbol{\epsilon}_{m+1} = \mathcal{S}_{\boldsymbol{n}_2}\boldsymbol{s} = \boldsymbol{\sigma} + \mathcal{S}\boldsymbol{\epsilon}_{m+1} = \mathcal{T}\boldsymbol{\epsilon}_{m+1},$$

mentre essendo $\boldsymbol{n}_1$ ed $\boldsymbol{n}_2$ ortogonali ad $\mathcal{S}S_{m+1}$ ed $\mathcal{S}R_m$ si ha inoltre

$$\mathcal{S}_{\boldsymbol{n}_2}\mathcal{S}_{\boldsymbol{n}_1}\boldsymbol{e}_i = \mathcal{S}\boldsymbol{e}_i = \mathcal{T}\boldsymbol{e}_i \qquad \text{per} \quad i \in (1,\ m+1)\,,$$

$$\mathcal{S}_{\boldsymbol{n}_2}\mathcal{S}_{\boldsymbol{n}_1}\mathcal{S}\boldsymbol{\epsilon}_i = \mathcal{S}\boldsymbol{\epsilon}_i = \mathcal{T}\boldsymbol{\epsilon}_i \qquad \text{per} \quad i \in (1,\ m)\,.$$

Questo complesso di relazioni mostrano che m non è il massimo valore raggiungibile da $m_s(\mathcal{T},\ \mathcal{S})$ quando $\mathcal{S}$ percorre G', in contraddizione con l'ipotesi di partenza. Perchè sussista quindi il sistema di condizioni

$$m = \operatorname*{Max}_{\mathcal{S}\in G'} m_s(\mathcal{T},\ \mathcal{S}), \qquad m < r\,,$$

l'unica possibilità che rimane è che si abbia

$$\dim_K V = 2m + 4\,.$$

cioè, n essendo pari ed r indicando la dimensione degli spazi totalmente singolari massimali, che si abbia

$$\dim_K V = 2r, \qquad m = r - 2\,.$$

5) Si dovranno ora distinguere due casi, a seconda che m sia diverso o meno dallo zero.

Si supponga dunque $m \neq 0$, cioè $r > 2$: quale vettore $\boldsymbol{u}$ si potrà prendere il vettore non singolare $\boldsymbol{e}_1 - \boldsymbol{\epsilon}_1$ e porre

$$\begin{aligned}
\boldsymbol{n}_1 &= \mathcal{S}\boldsymbol{e}_1 - \mathcal{S}\boldsymbol{\epsilon}_1 + \mathcal{S}\boldsymbol{e}_{m+1}, \\
\boldsymbol{n}_2 &= \mathcal{T}\boldsymbol{\epsilon}_{m+1} - \mathcal{S}\boldsymbol{\epsilon}_{m+1} - \mathcal{S}\boldsymbol{e}_1 + \mathcal{S}\boldsymbol{\epsilon}_1 - \mathcal{S}\boldsymbol{e}_{m+1}, \\
\boldsymbol{n}_3 &= \mathcal{S}\boldsymbol{e}_1 - \mathcal{S}\boldsymbol{\epsilon}_1, \\
\boldsymbol{n}_4 &= \mathcal{S}\boldsymbol{\epsilon}_1 - \mathcal{S}\boldsymbol{e}_1 - \mathcal{T}\boldsymbol{\epsilon}_{m+1} + \mathcal{S}\boldsymbol{\epsilon}_{m+1}.
\end{aligned}$$

Si ha

$$Q(\boldsymbol{n}_i) = -1, \qquad i \in (1, 4),$$

quindi tutti i vettori $\boldsymbol{n}_i$, $i \in (1, 4)$ sono non singolari. Questi vettori si possono scrivere nella forma

$$\begin{aligned}
\boldsymbol{n}_1 &= \mathcal{S}\boldsymbol{e}_1 - (\mathcal{S}\boldsymbol{\epsilon}_1 + \mathcal{S}\boldsymbol{e}_{m+1}), \\
\boldsymbol{n}_2 &= (\mathcal{S}\boldsymbol{\epsilon}_1 - \mathcal{S}\boldsymbol{e}_{m+1}) - (\mathcal{S}\boldsymbol{e}_1 - \mathcal{T}\boldsymbol{\epsilon}_{m+1} + \mathcal{S}\boldsymbol{\epsilon}_{m+1}), \\
\boldsymbol{n}_3 &= (\mathcal{S}\boldsymbol{e}_1 - \mathcal{T}\boldsymbol{\epsilon}_{m+1} + \mathcal{S}\boldsymbol{\epsilon}_{m+1}) - (\mathcal{S}\boldsymbol{\epsilon}_1 - \mathcal{T}\boldsymbol{\epsilon}_{m+1} + \mathcal{S}\boldsymbol{\epsilon}_{m+1}), \\
\boldsymbol{n}_4 &= (\mathcal{S}\boldsymbol{\epsilon}_1 - \mathcal{T}\boldsymbol{\epsilon}_{m+1} + \mathcal{S}\boldsymbol{\epsilon}_{m+1}) - \mathcal{S}\boldsymbol{e}_1,
\end{aligned}$$

e ciascuno dei due addendi nei quali è stato decomposto ognuno di questi vettori è singolare, per cui si può senz'altro applicare il Lemma A e scrivere

$$\mathcal{S}_{n_4}\mathcal{S}_{n_3}\mathcal{S}_{n_2}\mathcal{S}_{n_1}\mathcal{S}\boldsymbol{e}_1 = \mathcal{S}\boldsymbol{e}_1 = \mathcal{T}\boldsymbol{e}_1.$$

Similmente:

$$\begin{aligned}
-\boldsymbol{n}_1 &= \mathcal{S}\boldsymbol{\epsilon}_1 - (\mathcal{S}\boldsymbol{e}_1 + \mathcal{S}\boldsymbol{e}_{m+1}), \\
-\boldsymbol{n}_2 &= (\mathcal{S}\boldsymbol{e}_1 + \mathcal{S}\boldsymbol{e}_{m+1}) - (\mathcal{S}\boldsymbol{\epsilon}_1 - \mathcal{S}\boldsymbol{\epsilon}_{m+1} + \mathcal{T}\boldsymbol{\epsilon}_{m+1}), \\
-\boldsymbol{n}_3 &= (\mathcal{S}\boldsymbol{\epsilon}_1 - \mathcal{S}\boldsymbol{\epsilon}_{m+1} + \mathcal{T}\boldsymbol{\epsilon}_{m+1}) - (\mathcal{S}\boldsymbol{e}_1 - \mathcal{S}\boldsymbol{\epsilon}_{m+1} + \mathcal{T}\boldsymbol{\epsilon}_{m+1}), \\
-\boldsymbol{n}_4 &= (\mathcal{S}\boldsymbol{e}_1 - \mathcal{S}\boldsymbol{\epsilon}_{m+1} + \mathcal{T}\boldsymbol{\epsilon}_{m+1}) - \mathcal{S}\boldsymbol{\epsilon}_1,
\end{aligned}$$

è una decomposizione dei vettori $-\boldsymbol{n}_i$, $i \in (1, 4)$, con analoga proprietà e quindi,

sempre per il Lemma A,

$$\mathcal{S}_{n_4}\mathcal{S}_{n_3}\mathcal{S}_{n_2}\mathcal{S}_{n_1}\mathcal{S}\boldsymbol{\epsilon}_1 = \mathcal{S}\boldsymbol{\epsilon}_1 = \mathcal{T}\boldsymbol{\epsilon}_1 .$$

Poichè i vettori $\boldsymbol{n}_i$, $i \in (1, 4)$, appartengono allo spazio sotteso dai vettori $\mathcal{S}\boldsymbol{e}_1$, $\mathcal{S}\boldsymbol{\epsilon}_1$, $\mathcal{S}\boldsymbol{e}_{m+1}$, $\mathcal{S}\boldsymbol{\epsilon}_{m+1}$, $\mathcal{T}\boldsymbol{\epsilon}_{m+1}$, spazio che per definizione è ortogonale ai vettori $\mathcal{S}\boldsymbol{e}_i$, $\mathcal{S}\boldsymbol{\epsilon}_i$, $i \in (2, m)$, si ha ancora

$$\mathcal{S}_{n_4}\mathcal{S}_{n_3}\mathcal{S}_{n_2}\mathcal{S}_{n_1}\mathcal{S}\boldsymbol{e}_i = \mathcal{S}\boldsymbol{e}_i = \mathcal{T}\boldsymbol{e}_i , \qquad i \in (2, m) ,$$

$$\mathcal{S}_{n_4}\mathcal{S}_{n_3}\mathcal{S}_{n_2}\mathcal{S}_{n_1}\mathcal{S}\boldsymbol{\epsilon}_i = \mathcal{S}\boldsymbol{\epsilon}_i = \mathcal{T}\boldsymbol{\epsilon}_i , \qquad i \in (2, m) .$$

Similmente $\mathcal{S}\boldsymbol{e}_{m+1}$ è ortogonale ai vettori $\boldsymbol{n}_i$, $i \in (1, 4)$, e quindi

$$\mathcal{S}_{n_4}\mathcal{S}_{n_3}\mathcal{S}_{n_2}\mathcal{S}_{n_1}\mathcal{S}\boldsymbol{e}_{m+1} = \mathcal{S}\boldsymbol{e}_{m+1} = \mathcal{T}\boldsymbol{e}_{m+1} .$$

Infine la decomposizione dei vettori $\boldsymbol{n}_1$ ed $\boldsymbol{n}_2$ fornita dalle

$$-\boldsymbol{n}_1 = \mathcal{S}\boldsymbol{\epsilon}_{m+1} - (\mathcal{S}\boldsymbol{e}_1 - \mathcal{S}\boldsymbol{\epsilon}_1 + \mathcal{S}\boldsymbol{e}_{m+1} + \mathcal{S}\boldsymbol{\epsilon}_{m+1}) ,$$

$$-\boldsymbol{n}_2 = (\mathcal{S}\boldsymbol{e}_1 - \mathcal{S}\boldsymbol{\epsilon}_1 + \mathcal{S}\boldsymbol{e}_{m+1} + \mathcal{S}\boldsymbol{\epsilon}_{m+1}) - \mathcal{T}\boldsymbol{\epsilon}_{m+1} ,$$

è tale che ciascuno degli addendi è singolare, quindi, ancora per il Lemma A,

$$\mathcal{S}_{n_2}\mathcal{S}_{n_1}\mathcal{S}\boldsymbol{\epsilon}_{m+1} = \mathcal{T}\boldsymbol{\epsilon}_{m+1},$$

e siccome $\boldsymbol{n}_3$ ed $\boldsymbol{n}_4$ sono ortogonali a $\mathcal{T}\boldsymbol{\epsilon}_{m+1}$,

$$\mathcal{S}_{n_4}\mathcal{S}_{n_3}\mathcal{S}_{n_2}\mathcal{S}_{n_1}\mathcal{S}\boldsymbol{\epsilon}_{m+1} = \mathcal{T}\boldsymbol{\epsilon}_{m+1} .$$

Questa serie di risultati mostra che se si sceglie nel gruppo G' la trasformazione ortogonale

$$\mathcal{S}^* = \mathcal{S}_{n_4}\mathcal{S}_{n_3}\mathcal{S}_{n_2}\mathcal{S}_{n_1}\mathcal{S} ,$$

si giunge ad un risultato che non è compatibile con l'ipotesi che m sia il massimo valore che può assumere la funzione $m_S(\mathcal{T}, \mathcal{S})$ al variare di $\mathcal{S}$ in G': questa contraddizione implica che debba escludersi l'ipotesi di $m \neq 0$.

6) Rimane quindi da considerare, quale solo caso nel quale possano sussistere simultaneamente le due condizioni

$$m = \operatorname*{Max}_{\mathcal{S}\in G'} m_S(\mathcal{T}, \mathcal{S}) \quad \text{ed} \quad m < r,$$

il caso $m = 0$. Ma allora, essendo $m = r - 2$ ed $n = \dim_K V = 2r$, si ha

$$\dim_K V = 4, \qquad \dim_K S = 2 .$$

Si supponga che il corpo K sia diverso da $GF(2)$: allora K contiene almeno tre elementi, cioè esiste un elemento q di K diverso da 0 ed 1. Si potrà allora considerare il vettore

$$\boldsymbol{s} = \mathcal{S}\boldsymbol{\epsilon}_1 - q\mathcal{S}\boldsymbol{e}_1 + \boldsymbol{\sigma}^* + q\,\boldsymbol{\sigma},$$

e porre

$$\boldsymbol{n}_1 = \boldsymbol{s} - \mathcal{S}\boldsymbol{\epsilon}_1, \qquad \boldsymbol{n}_2 = \mathcal{S}\boldsymbol{\epsilon}_1 + \boldsymbol{\sigma} - \boldsymbol{s} = \boldsymbol{\sigma} - \boldsymbol{n}_1 .$$

Si ha

$$Q(\boldsymbol{n}_1) = q \neq 0 , \qquad Q(\boldsymbol{n}_2) = q - 1 \neq 0 ,$$

cioè i vettori $\boldsymbol{n}_1$ ed $\boldsymbol{n}_2$ sono non singolari. Inoltre $\boldsymbol{n}_1$ ed $\boldsymbol{n}_2$ sono ortogonali ad $\mathcal{S}\boldsymbol{\epsilon}_1$, quindi

$$\mathcal{S}_{n_2}\mathcal{S}_{n_1}\mathcal{S}\boldsymbol{e}_1 = \mathcal{S}\boldsymbol{e}_1,$$

ossia, per l'ipotesi iniziale,

$$\mathcal{S}_{n_2}\mathcal{S}_{n_1}\mathcal{S}\boldsymbol{e}_1 = \mathcal{T}\boldsymbol{e}_1 .$$

D'altra parte

$$-\boldsymbol{n}_1 = \mathcal{S}\boldsymbol{\epsilon}_1 - \boldsymbol{s}, \qquad -\boldsymbol{n}_2 = \boldsymbol{s} - (\mathcal{S}\boldsymbol{\epsilon}_1 + \boldsymbol{\sigma}) ,$$

quindi, ancora per il Lemma A,

$$\mathcal{S}_{n_1}\mathcal{S}\boldsymbol{\epsilon}_1 = \boldsymbol{s}, \qquad \mathcal{S}_{n_2}\mathcal{S}_{n_1}\mathcal{S}\boldsymbol{\epsilon}_1 = \mathcal{S}\boldsymbol{\epsilon}_1 + \boldsymbol{\sigma} = \mathcal{S}\boldsymbol{\epsilon}_1 + \mathcal{T}\boldsymbol{\epsilon}_1 - \mathcal{S}\boldsymbol{\epsilon}_1 = \mathcal{T}\boldsymbol{\epsilon}_1 .$$

Se quindi il corpo K ha più di due elementi si giunge ad un risultato che è incompatibile con il sistema di relazioni

$$m = \operatorname*{Max}_{\mathscr{S}\in G'} m_s(\mathscr{T}, \mathscr{S}), \qquad m = 0, \qquad r = 2, \qquad n = \dim_K V = 4;$$

ciò permette quindi di concludere che, escludendo il caso di $K = GF(2)$ con $\dim_K V = 4$, $\dim_K S = 2$, si ha *sempre* $m = r$.

7) Quest'ultimo risultato significa che il gruppo G' contiene almeno un elemento $\mathscr{S}$ tale che sia

$$\mathscr{S}\boldsymbol{x} = \mathscr{T}\boldsymbol{x} \qquad \text{per } \forall \boldsymbol{x} \in S \oplus R .$$

Se si suppone ora assegnata la trasformazione ortogonale $\mathscr{T}$ e si considera l'equazione

$$\mathscr{S}\boldsymbol{x} = \mathscr{T}\boldsymbol{x} ,$$

le soluzioni di questa equazione riempiono un sottospazio vettoriale contenuto in V che contiene necessariamente S e R: questo spazio delle soluzioni verrà segnato $V(\mathscr{T}, \mathscr{S})$ e si ha

$$V \supset V(\mathscr{T}, \mathscr{S}) \supset S \oplus R .$$

Sia ora

$$\nu = \operatorname*{Max}_{\mathscr{S}\in G'} \dim_K V(\mathscr{T}, \mathscr{S});$$

per dimostrare il teorema è sufficiente far vedere che $\nu = \dim_K V$. Per raggiungere questo scopo si supponga anzitutto che l'elemento $\mathscr{S}$ sia stato scelto nel gruppo G' in modo da raggiungere effettivamente il massimo ν, cioè si supponga che $\mathscr{S}$ sia tale che

$$\nu = \dim_K V(\mathscr{T}, \mathscr{S}) ,$$

e si supponga ancora che $\nu < \dim_K V$.

In virtù di questa ultima ipotesi si sa che esiste in V un vettore $\boldsymbol{y}$ tale che sia

$$\mathscr{S}\boldsymbol{y} \neq \mathscr{T}\boldsymbol{y}$$

e quindi si potrà porre

$$\boldsymbol{n} = \mathscr{T}\boldsymbol{y} - \mathscr{S}\boldsymbol{y} .$$

Il vettore $\boldsymbol{n}$ è non nullo ed è inoltre tale che per ogni $\boldsymbol{x} \in V(\mathscr{T}, \mathscr{S})$ sia

$$B(\boldsymbol{n}, \mathscr{S}\boldsymbol{x}) = B(\mathscr{T}\boldsymbol{y} - \mathscr{S}\boldsymbol{y}, \mathscr{S}\boldsymbol{x}) = B(\mathscr{T}\boldsymbol{y}, \mathscr{S}\boldsymbol{x}) - B(\mathscr{S}\boldsymbol{y}, \mathscr{S}\boldsymbol{x})$$

$$= B(\mathscr{T}\boldsymbol{y}, \mathscr{T}\boldsymbol{x}) - B(\mathscr{S}\boldsymbol{y}, \mathscr{S}\boldsymbol{x}) = B(\boldsymbol{y}, \boldsymbol{x}) - B(\boldsymbol{y}, \boldsymbol{x}) = 0$$

e quindi $\boldsymbol{n}$ è ortogonale ad $\mathscr{S}V(\mathscr{T}, \mathscr{S})$. Poichè $V(\mathscr{T}, \mathscr{S}) \supset S \oplus R$, $\boldsymbol{n}$ è parimenti ortogonale ad $\mathscr{S}(S \oplus R)$ e siccome S è uno spazio totalmente singolare, $S \oplus R$, e di conseguenza $\mathscr{S}(S \oplus R)$ è non isotropo. Si ha dunque che $\boldsymbol{n} \in [\mathscr{S}(S \oplus R)]^0$, cioè $\boldsymbol{n}$ è non singolare. La simmetria $\mathscr{S}_n$ definita mediante questo vettore lascia fissi tutti gli elementi di $\mathscr{S}V(\mathscr{T}, \mathscr{S})$, cioè uno spazio vettoriale di dimensione ν, ma ancora

$$\begin{aligned}
\mathscr{S}_n \mathscr{S}\boldsymbol{y} &= \mathscr{S}\boldsymbol{y} - Q^{-1}(\boldsymbol{n})\, B(\boldsymbol{n}, \mathscr{S}\boldsymbol{y})\, \boldsymbol{n} = \mathscr{S}\boldsymbol{y} - Q^{-1}(\boldsymbol{n})\, B(\mathscr{T}\boldsymbol{y} - \mathscr{S}\boldsymbol{y}, \mathscr{S}\boldsymbol{y})\boldsymbol{n} \\
&= \mathscr{S}\boldsymbol{y} - Q^{-1}(\boldsymbol{n})\, [Q(\mathscr{T}\boldsymbol{y}) - Q(\mathscr{T}\boldsymbol{y} - \mathscr{S}\boldsymbol{y}) - Q(\mathscr{S}\boldsymbol{y})]\, \boldsymbol{n} \\
&= \mathscr{S}\boldsymbol{y} - Q^{-1}(\boldsymbol{n})\, Q(\mathscr{T}\boldsymbol{y} - \mathscr{S}\boldsymbol{y})\boldsymbol{n} = \mathscr{S}\boldsymbol{y} + Q^{-1}(\boldsymbol{n})\, Q(\boldsymbol{n})\boldsymbol{n} \\
&= \mathscr{S}\boldsymbol{y} + \boldsymbol{n} = \mathscr{T}\boldsymbol{y}\,,
\end{aligned}$$

per cui

$$V(\mathscr{T}, \mathscr{S}_n \mathscr{S}) \geqslant V(\mathscr{T}, \mathscr{S}) \oplus K\boldsymbol{y}$$

ovvero

$$\dim_K V(\mathscr{T}, \mathscr{S}_n\mathscr{S}) = \nu + 1\,,$$

e siccome questo risultato è in contraddizione con l'ipotesi di ν massimo non può essere $\nu < \dim_K V$.

Si ha dunque

$$\nu = \dim_K V\,,$$

e con ciò risulta dimostrato il teorema.

Parte seconda.

10. - Le pseudo-simmetrie.

Dato uno spazio vettoriale V dotato di una forma quadratica non degenere Q, sia $\boldsymbol{\sigma} \in V$ un suo vettore singolare: $\boldsymbol{\sigma}$ definisce allora uno spazio totalmente singolare $S = K\boldsymbol{\sigma}$ di cui

$$S^0 = \{\, \boldsymbol{x} \in V \mid B(\boldsymbol{x}, \boldsymbol{\sigma}) = 0 \,\}$$

è lo spazio coniugato e si ha $S \subset S^0 \subset V$.

Per la decomposizione di WITT, V contiene allora un vettore singolare $\boldsymbol{\sigma}^*$ tale che

$$B(\boldsymbol{\sigma}, \boldsymbol{\sigma}^*) = 1\,; \tag{1}$$

quest'ultima proprietà di $\boldsymbol{\sigma}^*$ mostra che $\boldsymbol{\sigma}^* \notin S^0$, e quindi

$$V = S^0 \oplus K\boldsymbol{\sigma}^*. \tag{2}$$

Si scelgano ora in S^0

a) uno spazio U tale che

$$\dim_K U = \dim_K S^0 - 1;$$

b) un vettore $\boldsymbol{\omega}$ tale che

$$\boldsymbol{\omega} \in S^0, \quad \boldsymbol{\omega} \notin U, \quad \boldsymbol{\omega} + \boldsymbol{\sigma} \notin U. \tag{3}$$

Sotto queste ipotesi *esiste una trasformazione ortogonale* $\mathscr{P}$ *di* V *tale che*

$$\mathscr{P}\boldsymbol{\omega} = \boldsymbol{\omega} + \boldsymbol{\sigma}, \tag{4}$$

$$\mathscr{P}\boldsymbol{u} = \boldsymbol{u} \quad \text{per} \quad \forall \boldsymbol{u} \in U. \tag{5}$$

Per dimostrare questa affermazione, si osservi anzitutto che la scelta di $\boldsymbol{\omega}$ fatta secondo la (3) implica che

$$S^0 = U \oplus K\boldsymbol{\omega}, \tag{6}$$

per cui ogni vettore di S^0 si potrà scrivere nella forma

$$\boldsymbol{y} = \boldsymbol{u} + h\,\boldsymbol{\omega},$$

$\boldsymbol{u}$ essendo un opportuno elemento di U ed h un opportuno elemento di K. Si verifica immediatamente che, se esiste un'applicazione $\mathscr{P}$ di V in V soddisfacente alle (4) e (5), che sia ortogonale, la sua restrizione ad S^0 sarà parimenti ortogonale cioè

$$Q(\mathscr{P}\boldsymbol{y}) = Q(\boldsymbol{y}).$$

Riunendo poi le (2) e (6) risulta

$$V = U \oplus K\boldsymbol{\omega} \oplus K\boldsymbol{\sigma}^*,$$

e quindi perchè $\mathscr{P}$ sia una trasformazione ortogonale di V è necessario e suffi-

ciente che siano soddisfatte le condizioni

$$Q(\mathscr{P}\boldsymbol{\sigma}^*) = Q(\boldsymbol{\sigma}^*)\,, \tag{7}$$

$$B(\mathscr{P}\boldsymbol{\sigma}^*,\ \mathscr{P}\boldsymbol{\omega}) = B(\boldsymbol{\sigma}^*,\ \boldsymbol{\omega})\,, \tag{8}$$

$$B(\mathscr{P}\boldsymbol{\sigma}^*,\ \mathscr{P}\boldsymbol{u}) = B(\boldsymbol{\sigma}^*,\ \boldsymbol{u}) \qquad \text{per } \forall \boldsymbol{u} \in U\,. \tag{9}$$

L'ultima di queste, tenuto conto della (5), si riscrive

$$B(\mathscr{P}\boldsymbol{\sigma}^* - \boldsymbol{\sigma}^*,\ \boldsymbol{u}) = 0 \qquad \text{per } \forall \boldsymbol{u} \in U\,,$$

cioè

$$\mathscr{P}\boldsymbol{\sigma}^* - \boldsymbol{\sigma}^* \in U^0. \tag{10}$$

Si osservi però che

$$S^0 = (K\boldsymbol{\sigma})^0 \supset U\,,$$

quindi $U^0 \supset K\boldsymbol{\sigma}$, cioè $\boldsymbol{\sigma} \in U^0$.

Inoltre, tenendo presente il gioco delle dimensioni, si ha

$$(U \oplus K\boldsymbol{\sigma}^*)^0 = K\boldsymbol{v}.$$

ovvero

$$U^0 \cap (K\boldsymbol{\sigma}^*)^0 = K\boldsymbol{v}\,,$$

cioè

$$\boldsymbol{v} \in U^0, \quad \boldsymbol{v} \perp \boldsymbol{\sigma}^*\,.$$

Da questa ultima relazione, tenuto conto della (1), segue che

$$\boldsymbol{v} \notin K\boldsymbol{\sigma}$$

per cui

$$U^0 = K\boldsymbol{\sigma} \oplus K\boldsymbol{v}\,.$$

Dalla (10), quindi, si deduce che

$$\mathscr{P}\boldsymbol{\sigma}^* = \boldsymbol{\sigma}^* + a\,\boldsymbol{\sigma} + b\,\boldsymbol{v}, \qquad a,\ b \in K\,.$$

Utilizzando ora le (7) ed (8), si trovano per a e b le due equazioni

$$a + a\,b\,B(\boldsymbol{\sigma},\ \boldsymbol{v}) + b^2\,Q(\boldsymbol{v}) = 0,$$

$$b\,B(\boldsymbol{\omega},\ \boldsymbol{v}) + b\,B(\boldsymbol{\sigma},\ \boldsymbol{v}) + 1 = 0\,,$$

che si riscrivono

$$b\,B(\boldsymbol{\omega} + \boldsymbol{\sigma},\ \boldsymbol{v}) + 1 = 0\,, \tag{11}$$

$$a\,bB(\boldsymbol{\omega},\ \boldsymbol{v}) - b^2\,Q(\boldsymbol{v}) = 0\,. \tag{12}$$

Poichè

$$V = U \oplus K\boldsymbol{\omega} \oplus K\boldsymbol{\sigma}^*$$

e $\boldsymbol{v} \perp U$, $\boldsymbol{v} \perp \boldsymbol{\sigma}^*$, il vettore $\boldsymbol{v}$ non può essere ortogonale ad $\boldsymbol{\omega}$: infatti, se lo fosse esisterebbe in V un vettore non nullo, $\boldsymbol{v}$ stesso, ortogonale a tutti i vettori di V, cioè V^0 conterrebbe almeno un vettore non nullo e B, e di conseguenza Q, sarebbe degenere, contrariamente all'ipotesi. Similmente, tenuto conto della (3), si può scrivere

$$V = U \oplus K(\boldsymbol{\omega} + \boldsymbol{\sigma}) \oplus K\boldsymbol{\sigma}^*,$$

ed il ragionamento precedente porta a concludere che $\boldsymbol{v}$ non può essere ortogonale ad $\boldsymbol{\omega} + \boldsymbol{\sigma}$. Segue da ciò che

$$B(\boldsymbol{\omega},\ \boldsymbol{v}) \neq 0, \qquad B(\boldsymbol{\omega} + \boldsymbol{\sigma},\ \boldsymbol{v}) \neq 0\,,$$

per cui il sistema costituito dalle equazioni (11) e (12) è sempre risolubile, e precisamente si ha

$$a = -\,Q(\boldsymbol{v})\,B^{-1}(\boldsymbol{\omega} + \boldsymbol{\sigma},\ \boldsymbol{v})\,B^{-1}(\boldsymbol{\omega},\ \boldsymbol{v}), \qquad b = -\,B^{-1}(\boldsymbol{\omega} + \boldsymbol{\sigma},\ \boldsymbol{v})\,.$$

L'applicazione ortogonale $\mathscr{P}$ esiste dunque effettivamente e la sua espressione esplicita è fornita dalle seguenti equazioni:

$$\mathscr{P}\boldsymbol{u} = \boldsymbol{u} \qquad \text{per } \forall \boldsymbol{u} \in U\,,$$

$$\mathscr{P}\boldsymbol{\omega} = \boldsymbol{\omega} + \boldsymbol{\sigma}\,,$$

$$\mathscr{P}\boldsymbol{\sigma}^* = \boldsymbol{\sigma}^* - Q(\boldsymbol{v})\, B^{-1}(\boldsymbol{\omega} + \boldsymbol{\sigma},\, \boldsymbol{v})\, B^{-1}(\boldsymbol{\omega},\, \boldsymbol{v})\, \boldsymbol{\sigma} - B^{-1}(\boldsymbol{\omega} + \boldsymbol{\sigma},\, \boldsymbol{v})\, \boldsymbol{v}\,.$$

Si osservi che l'applicazione ortogonale $\mathscr{P}$ ottenuta estendendo una trasformazione ortogonale particolare definita su S^0 a tutto lo spazio V, risulta definita in V in maniera *unica*, purchè siano assegnati U ed $\boldsymbol{\omega}$. Vale a dire che ogni $\mathscr{P}$ corrisponde ad una scelta di $\boldsymbol{\sigma}$, di U e di $\boldsymbol{\omega}$. Se si sostituisce a $\boldsymbol{\sigma}$ un qualsiasi altro elemento di S, ad esempio $h\,\boldsymbol{\sigma}$, $h \in K$, $h \neq 0, 1$, l'applicazione $\mathscr{P}$ rimane la stessa, fermi restando U ed $\boldsymbol{\omega}$: sarà soltanto necessario, nella esposizione precedente, sostituire a $\boldsymbol{\sigma}^*$ il vettore $h^{-1}\,\boldsymbol{\sigma}^*$ perchè sia soddisfatta la (1).

$\mathscr{P}$ gode inoltre della proprietà di lasciare immutati tutti gli elementi di U, cioè di uno spazio vettoriale di dimensione $\dim_K V - 2$ contenuto in V.

Le applicazioni ortogonali ottenute in questa maniera verranno nel seguito indicate con la notazione $\mathscr{P}_{\sigma,U,\omega}$ e chiamate *pseudosimmetrie.*

Si osservi ancora che se al vettore $\boldsymbol{\omega}$ si sostituisce un vettore $\boldsymbol{\omega}^*$ tale che

$$\boldsymbol{\omega}^* = \boldsymbol{\omega} + \boldsymbol{u}_0,$$

con $\boldsymbol{u}_0 \in U$, la pseudo-simmetria $\mathscr{P}_{\sigma,U,\omega}$ non cambia. Invero

$$\mathscr{P}_{\sigma,U,\omega}\,\boldsymbol{\omega}^* = \mathscr{P}_{\sigma,U,\omega}\,(\boldsymbol{\omega} + \boldsymbol{u}_0) = \mathscr{P}_{\sigma,U,\omega}\,\boldsymbol{\omega} + \mathscr{P}_{\sigma,U,\omega}\,\boldsymbol{u}_0$$
$$= \boldsymbol{\omega} + \boldsymbol{\sigma} + \boldsymbol{u}_0 = \boldsymbol{\omega}^* + \boldsymbol{\sigma}\,,$$

$$\mathscr{P}_{\sigma,U,\omega}\,\boldsymbol{u} = \boldsymbol{u} \qquad \text{per } \forall \boldsymbol{u} \in U\,,$$

e, siccome $\boldsymbol{v} \perp U$,

$$B(\boldsymbol{\omega}^* + \boldsymbol{\sigma},\, \boldsymbol{v}) = B(\boldsymbol{\omega} + \boldsymbol{u}_0 + \boldsymbol{\sigma},\, \boldsymbol{v}) = B(\boldsymbol{\omega} + \boldsymbol{\sigma},\, \boldsymbol{v})\,,$$

$$B(\boldsymbol{\omega}^*,\, \boldsymbol{v}) = B(\boldsymbol{\omega} + \boldsymbol{u}_0,\, \boldsymbol{v}) = B(\boldsymbol{\omega},\, \boldsymbol{v})\,,$$

per cui

$$\mathscr{P}_{\sigma,U,\omega}\,\boldsymbol{\sigma}^* = \boldsymbol{\sigma}^* - Q(\boldsymbol{v})\, B^{-1}(\boldsymbol{\omega}^* + \boldsymbol{\sigma},\, \boldsymbol{v})\, B^{-1}(\boldsymbol{\omega}^*,\, \boldsymbol{v})\, \boldsymbol{\sigma} - B^{-1}(\boldsymbol{\omega}^* + \boldsymbol{\sigma},\, \boldsymbol{v})\, \boldsymbol{v},$$

cioè

$$\mathscr{P}_{\sigma,U,\omega} = \mathscr{P}_{\sigma,U,\omega^*} .$$

Si indicherà con G'' il gruppo generato dalla totalità delle simmetrie e delle pseudo-simmetrie definite in V: si ha evidentemente $G' \subseteq G'' \subseteq G$.

11. - Il Teorema di Witt.

Sia R un sotto-spazio vettoriale di V ed $\mathscr{H}$ denoti una applicazione omomorfa di R in V, tale che sia

$$Q(\mathscr{H}\boldsymbol{x}) = Q(\boldsymbol{x}) \qquad \text{per } \forall\, \boldsymbol{x} \in R: \tag{1}$$

$\mathscr{H}$ si dice allora *omomorfismo metrico* in V definito su R. Se, oltre alla condizione (1), $\mathscr{H}$ soddisfa ancora la condizione

$$\operatorname{Ker} \mathscr{H} = \{ \boldsymbol{x} \in V \mid \mathscr{H}\boldsymbol{x} = 0 \} = \{ 0 \},$$

si dice che $\mathscr{H}$ è un *isomorfismo metrico.*

Se B è la forma bilineare aggiunta a Q, dalle definizioni precedenti segue che

$$B(\mathscr{H}\boldsymbol{x},\ \mathscr{H}\boldsymbol{y}) = B(\boldsymbol{x},\ \boldsymbol{y}) \qquad \text{per } \forall \boldsymbol{x},\ \boldsymbol{y} \in R .$$

Poste queste definizioni preliminari si può enunciare il

Teorema di Witt. *Sia V uno spazio vettoriale di dimensione finita n, dotato di forma quadratica Q non degenere e sia R un sottospazio di V. Ogni isomorfismo metrico definito su R si può estendere a tutto lo spazio V mediante una opportuna scelta di un elemento appartenente a G''.*

Dimostrazione. Sia $\mathscr{H}$ l'isomorfismo metrico definito su R e sia $\mathscr{T}$ un qualsiasi elemento del gruppo G'': posto

$$R(\mathscr{T},\ \mathscr{H}) = \{ \boldsymbol{r} \in R \mid \mathscr{T}\boldsymbol{r} - \mathscr{H}\boldsymbol{r} = 0 \} \subset R,$$

sia ancora

$$\nu = \operatorname*{Max}_{\mathscr{T} \in G''} \dim_K R(\mathscr{T}, \mathscr{H}) .$$

Il teorema di Witt è dimostrato qualora risulti che $\nu = \dim_K R$, poichè in tal caso $R(\mathscr{T}, \mathscr{H}) = R$.

Sia $\mathscr{T}$ appunto uno di quegli elementi di G'' che permettono di raggiungere effettivamente il valore ν: sarà quindi lecito scrivere

$$\nu = \dim_K R(\mathscr{T},\ \mathscr{H}) .$$

Si supponga $\nu < \dim_K R$: ciò significa che esiste almeno un vettore $\boldsymbol{y}$ tale che

$$\boldsymbol{y} \in R, \qquad \boldsymbol{y} \notin R(\mathscr{T}, \mathscr{H}),$$

e quindi si potrà definire il vettore $\boldsymbol{\sigma}$ come

$$\boldsymbol{\sigma} = \mathscr{H}\boldsymbol{y} - \mathscr{T}\boldsymbol{y} \neq 0 .$$

Il vettore $\boldsymbol{\sigma}$ è ortogonale allo spazio $\mathscr{T}R(\mathscr{T}, \mathscr{H})$: invero, se $\boldsymbol{r} \in R(\mathscr{T}, \mathscr{H}) \subset R$, si ha

$$\begin{aligned} B(\mathscr{T}\boldsymbol{r}, \boldsymbol{\sigma}) &= B(\mathscr{T}\boldsymbol{r}, \mathscr{H}\boldsymbol{y} - \mathscr{T}\boldsymbol{y}) = B(\mathscr{T}\boldsymbol{r}, \mathscr{H}\boldsymbol{y}) - B(\mathscr{T}\boldsymbol{r}, \mathscr{T}\boldsymbol{y}) \\ &= B(\mathscr{H}\boldsymbol{r}, \mathscr{H}\boldsymbol{y}) - B(\mathscr{T}\boldsymbol{r}, \mathscr{T}\boldsymbol{y}) = B(\boldsymbol{r}, \boldsymbol{y}) - B(\boldsymbol{r}, \boldsymbol{y}) = 0, \end{aligned}$$

e quindi

$$\mathscr{T}R(\mathscr{T}, \mathscr{H}) \subseteq (K\boldsymbol{\sigma})^0.$$

Conseguentemente, se il vettore $\boldsymbol{\sigma}$ è non singolare, la simmetria $\mathscr{S}_\sigma$ lascia fissi tutti gli elementi di $\mathscr{T}R(\mathscr{T}, \mathscr{H})$, cioè $\mathscr{S}_\sigma\mathscr{T}$ lascia fissi tutti gli elementi di $R(\mathscr{T}, \mathscr{H})$. D'altra parte, per il Lemma A,

$$\mathscr{S}_\sigma\mathscr{T}\boldsymbol{y} = \mathscr{H}\boldsymbol{y},$$

e quindi l'equazione

$$\mathscr{S}_\sigma\mathscr{T}\boldsymbol{x} = \mathscr{H}\boldsymbol{x}$$

ammette per soluzioni tutti gli elementi dello spazio vettoriale $R(\mathscr{T}, \mathscr{H})$ e tutto lo spazio $K\boldsymbol{y}$, cioè le soluzioni di questa equazione riempiono uno spazio vettoriale $R(\mathscr{T}, \mathscr{H}) \oplus K\boldsymbol{y}$ che ha dimensione $\nu + 1$: questo è in contraddizione con l'ipotesi di massimalità di ν.

Il vettore $\boldsymbol{\sigma}$ deve quindi essere singolare: in tal caso, però, $\mathscr{T}\boldsymbol{y}$ è ortogonale a $\boldsymbol{\sigma}$ perchè

$$Q(\mathscr{T}\boldsymbol{y} + \boldsymbol{\sigma}) = Q(\mathscr{H}\boldsymbol{y}) = Q(\boldsymbol{y}),$$

$$Q(\mathscr{T}\boldsymbol{y} + \boldsymbol{\sigma}) = Q(\mathscr{T}\boldsymbol{y}) + Q(\boldsymbol{\sigma}) + B(\mathscr{T}\boldsymbol{y}, \boldsymbol{\sigma}) = Q(\boldsymbol{y}) + B(\mathscr{T}\boldsymbol{y}, \boldsymbol{\sigma}),$$

quindi

$$B(\mathscr{T}\boldsymbol{y}, \boldsymbol{\sigma}) = 0 .$$

Il vettore è quindi ortogonale sia a $\mathscr{T}R(\mathscr{T}, \mathscr{H})$, sia a $\mathscr{T}\boldsymbol{y}$ e quindi sia lo spazio $\mathscr{T}R(\mathscr{T}, \mathscr{H})$ che il vettore $\mathscr{T}\boldsymbol{y}$ appartengono ad $S^0 = (K\boldsymbol{\sigma})^0$. Si può quindi scegliere in S^0 uno spazio subordinato U, la cui dimensione soddisfa la condizione

$$\dim_K U = \dim_K S^0 - 1 ,$$

tale che

$$\mathscr{T}R(\mathscr{T}, \mathscr{H}) \subset U, \qquad \mathscr{T}\boldsymbol{y} \notin U .$$

Si consideri ora la pseudo-simmetria $\mathscr{P}_{\sigma,U,\mathscr{T}\boldsymbol{y}}$: questa pseudo-simmetria lascia fissi tutti gli elementi di U e quindi

$$\mathscr{P}_{\sigma,U,\mathscr{T}\boldsymbol{y}}\boldsymbol{r} = \boldsymbol{r} \qquad \text{per } \forall \boldsymbol{r} \in \mathscr{T}R(\mathscr{T}, \mathscr{H}) \subset U,$$

ed inoltre è tale che

$$\mathscr{P}_{\sigma,U,\mathscr{T}\boldsymbol{y}}\,\mathscr{T}\boldsymbol{y} = \mathscr{T}\boldsymbol{y} + \boldsymbol{\sigma} = \mathscr{H}\boldsymbol{y} .$$

Conseguentemente l'equazione

$$\mathscr{P}_{\sigma,U,\mathscr{T}\boldsymbol{y}}\,\mathscr{T}\boldsymbol{x} = \mathscr{H}\boldsymbol{x}$$

ammette per soluzioni tutti gli elementi dello spazio $R(\mathscr{T}, \mathscr{H})$ e tutto lo spazio $K\boldsymbol{y}$, cioè ancora le soluzioni di questa equazione riempiono uno spazio vettoriale di dimensione superiore a ν, contrariamente al supposto. Si deve quindi scartare l'ipotesi di $\nu < \dim_K R$ e con ciò il teorema è dimostrato.

Corollario. *Se lo spazio vettoriale V ha dimensione finita e la forma quadratica Q è non degenere, il gruppo G'' coincide con il gruppo G.*

Per dimostrare il Corollario, basta prendere, nella dimostrazione che precede, quale spazio R tutto lo spazio V e quale isomorfismo metrico una qualsiasi applicazione ortogonale, per concludere, secondo il Teorema di WITT, che esiste un elemento di G'' che coincide su tutto V con l'applicazione ortogonale considerata: con questa osservazione risulta dimostrato l'asserto.

12. - Seconda dimostrazione del Teorema di Cartan e Dieudonné.

Dal Corollario del Teorema di WITT segue che

$$G' \subseteq G'' \equiv G$$

e quindi la seconda dimostrazione del teorema di CARTAN e DIEUDONNÉ si ot-

terrà dimostrando che assegnato un elemento $\mathscr{P}_{\sigma,U,\omega} = \mathscr{P}$ del gruppo G'', qualunque, questo risulta elemento del gruppo G'.

A seconda della locazione del vettore $\boldsymbol{\sigma}$ si distingueranno due casi nella dimostrazione.

Caso A) $\boldsymbol{\sigma} \notin U$.

Poichè il vettore $\boldsymbol{\sigma}$ è comunque un vettore singolare, si ha ancora $Q(\boldsymbol{\sigma}) = 0$, $B(\boldsymbol{\sigma}, \boldsymbol{\sigma}) = 0$ e quindi

$$\boldsymbol{\sigma} \in (K\boldsymbol{\sigma})^0 = S^0,$$

per cui si potrà scrivere

$$S^0 = U \oplus K\boldsymbol{\sigma},$$

essendo per ipotesi $\boldsymbol{\sigma}$ esterno ad U. Inoltre, è lecito sostituire al vettore $\boldsymbol{\omega}$ che definisce la pseudo-simmetria $\mathscr{P}$ un vettore $h\boldsymbol{\sigma}$: $\mathscr{P}$ rimane invariata. Infatti, per la decomposizione di S^0 data sopra, un qualunque elemento di S^0, e quindi anche $\boldsymbol{\omega}$, potrà scriversi

$$\boldsymbol{\omega} = \boldsymbol{u} + k\,\boldsymbol{\sigma},$$

essendo $\boldsymbol{u}$ un opportuno elemento di U e $k \neq 0$ (chè altrimenti non sarebbe rispettata l'ipotesi che $\boldsymbol{\omega} \notin U$) un opportuno elemento di K. In queste condizioni

$$\mathscr{P}\boldsymbol{\omega} = \boldsymbol{\omega} + \boldsymbol{\sigma} = \boldsymbol{u} + k\,\boldsymbol{\sigma} + \boldsymbol{\sigma} = \boldsymbol{u} + (k+1)\boldsymbol{\sigma}$$

ed ancora deve essere $k + 1 \neq 0$, perchè diversamente la pseudo-simmetria $\mathscr{P}$ farebbe corrispondere ad $\boldsymbol{\omega}$ un elemento di U ed al vettore $\boldsymbol{\omega} - \boldsymbol{u} \neq 0$ corrisponderebbe per $\mathscr{P}$ il vettore nullo, contro l'ipotesi che il nucleo delle trasformazioni ortogonali è vuoto. D'altra parte

$$\mathscr{P}\boldsymbol{\omega} = \mathscr{P}(\boldsymbol{u} + k\,\boldsymbol{\sigma}) = \mathscr{P}\boldsymbol{u} + k\,\mathscr{P}\boldsymbol{\sigma} = \boldsymbol{u} + k\,\mathscr{P}\boldsymbol{\sigma},$$

e quindi

$$\mathscr{P}(k\,\boldsymbol{\sigma}) = k\,\boldsymbol{\sigma} + \boldsymbol{\sigma}.$$

Si consideri ora il vettore $k\boldsymbol{\sigma}$:

$$k\,\boldsymbol{\sigma} \notin U \qquad \text{perchè } \boldsymbol{\sigma} \notin U,\ k \neq 0,$$

$$k\,\boldsymbol{\sigma} + \boldsymbol{\sigma} \notin U \qquad \text{perchè } \boldsymbol{\sigma} \notin U,\ k + 1 \neq 0,$$

$$\mathscr{P}(k\,\boldsymbol{\sigma}) = k\,\boldsymbol{\sigma} + \boldsymbol{\sigma},$$

quindi $k\,\boldsymbol{\sigma}$ gode di tutte le proprietà di $\boldsymbol{\omega}$ e si può sostituire ad $\boldsymbol{\omega}$ senza modificare la pseudo-simmetria $\mathscr{P}$.

Inoltre

$$U^0 \notin S^0.$$

Infatti, se fosse $U^0 \subseteq S^0$, sarebbe $(U^0)^0 = U \supseteq (S^0)^0 = S = K\boldsymbol{\sigma}$, per cui sarebbe $\boldsymbol{\sigma} \in U$, contrariamente all'ipotesi. U^0 ha ovviamente dimensione 2, contiene inoltre $\boldsymbol{\sigma}$ perchè $\boldsymbol{\sigma}$ è ortogonale ad S^0 ed U è contenuto in S^0. Esiste dunque in U^0 un vettore $\boldsymbol{\sigma}^*$ tale che

$$B(\boldsymbol{\sigma},\ \boldsymbol{\sigma}^*) = 1,$$

e quindi

$$\boldsymbol{\sigma}^* \notin (K\boldsymbol{\sigma})^0 = S^0.$$

Si ha dunque

$$V = U \oplus K\boldsymbol{\sigma} \oplus K\boldsymbol{\sigma}^*,$$

$$U^0 = K\boldsymbol{\sigma} \oplus K\boldsymbol{\sigma}^*.$$

Si potrà sempre supporre il vettore $\boldsymbol{\sigma}^*$ singolare. Invero, se ciò non fosse, basterebbe porre $\boldsymbol{\sigma}_1^* = \boldsymbol{\sigma}^* + h\,\boldsymbol{\sigma}$, $h \in K$, $h \neq 0$. Allora

$$B(\boldsymbol{\sigma},\ \boldsymbol{\sigma}_1^*) = 1, \qquad \boldsymbol{\sigma}_1^* \in U^0 \notin S^0, \qquad Q(\boldsymbol{\sigma}_1^*) = Q(\boldsymbol{\sigma}^*) + h,$$

e quindi è sufficiente scegliere in K, $h = -Q(\boldsymbol{\sigma}^*)$ per avere $Q(\boldsymbol{\sigma}_1^*) = 0$ ed ovviamente il vettore $\boldsymbol{\sigma}_1^*$ potrà essere chiamato a sostituire $\boldsymbol{\sigma}^*$ senza che nulla sia modificato.

Si considerino ora le proprietà della pseudo-simmetria $\mathscr{P}$: si ha

$$\mathscr{P}\boldsymbol{u} = \boldsymbol{u} \qquad \text{per } \forall \boldsymbol{u} \in U;$$

$$\mathscr{P}\boldsymbol{\sigma} = \frac{k+1}{k}\,\boldsymbol{\sigma} = p\,\boldsymbol{\sigma}, \qquad p \in K,\ p \neq 0\,.$$

Inoltre, poichè $V = U \oplus U^0$ e $\mathscr{P}U = U$, si avrà $\mathscr{P}U^0 = U^0$ e quindi

$$\mathscr{P}\boldsymbol{\sigma}^* = a\,\boldsymbol{\sigma} + b\,\boldsymbol{\sigma}^*.$$

Ma

$$B(\mathscr{P}\boldsymbol{\sigma}^*,\ \mathscr{P}\boldsymbol{\sigma}) = B(a\,\boldsymbol{\sigma} + b\,\boldsymbol{\sigma}^*,\ p\,\boldsymbol{\sigma}) = b\,p = 1 \qquad \text{quindi } b = p^{-1},$$

$$Q(\mathscr{P}\boldsymbol{\sigma}^*) = a\,b = 0 \qquad \text{quindi } a = 0\,,$$

per cui

$$\mathscr{P}\boldsymbol{\sigma}^* = p^{-1}\,\boldsymbol{\sigma}^*.$$

Si considerino ora i vettori

$$\boldsymbol{n}_1 = p\;\boldsymbol{\sigma}^* - \boldsymbol{\sigma}, \qquad \boldsymbol{n}_2 = \boldsymbol{\sigma} - \boldsymbol{\sigma}^*;$$

si ha

$$Q(\boldsymbol{n}_1) = Q(p\;\boldsymbol{\sigma}^* - \boldsymbol{\sigma}) = -p \neq 0, \qquad Q(\boldsymbol{n}_2) = Q(\boldsymbol{\sigma} - \boldsymbol{\sigma}^*) = -1 \neq 0\,,$$

cioè i vettori $\boldsymbol{n}_1$ ed $\boldsymbol{n}_2$ sono ambedue non singolari. Inoltre questi due vettori appartengono allo spazio U^0 e sono quindi ortogonali ad U, per cui le simmetrie definite mediante questi vettori lasciano fissi tutti gli elementi di U, e così pure il prodotto di tali simmetrie. Si può dunque senz'altro scrivere

$$\mathscr{S}_{n_2}\mathscr{S}_{n_1}\boldsymbol{u} = \boldsymbol{u} \qquad \text{per } \forall \boldsymbol{u} \in U\,.$$

Inoltre, i vettori nei quali si decompongono $\boldsymbol{n}_1$ ed $\boldsymbol{n}_2$ sono tutti singolari per cui, applicando il Lemma A, si ha

$$\mathscr{S}_{n_1}\boldsymbol{\sigma} = p\;\boldsymbol{\sigma}^*, \qquad \mathscr{S}_{n_2}\boldsymbol{\sigma}^* = \boldsymbol{\sigma}\,,$$

quindi

$$\mathscr{S}_{n_2}\mathscr{S}_{n_1}\boldsymbol{\sigma} = \mathscr{S}_{n_2}\,p\;\boldsymbol{\sigma}^* = p\;\boldsymbol{\sigma}\,.$$

Infine, sempre per il Lemma A,

$$\mathscr{S}_{n_1}\,p\;\boldsymbol{\sigma}^* = \boldsymbol{\sigma}, \qquad \mathscr{S}_{n_2}\boldsymbol{\sigma} = \boldsymbol{\sigma}^*,$$

quindi

$$\mathscr{S}_{n_1}\boldsymbol{\sigma}^* = p^{-1}\,\boldsymbol{\sigma}, \qquad \mathscr{S}_{n_2}\mathscr{S}_{n_1}\boldsymbol{\sigma}^* = p^{-1}\,\boldsymbol{\sigma}^*\,.$$

Il prodotto delle simmetrie $\mathscr{S}_{n_1}$ ed $\mathscr{S}_{n_2}$ opera quindi esattamente come la pseudo-simmetria $\mathscr{P}$ cioè $\mathscr{S}_{n_2}\mathscr{S}_{n_1}$ coincide con essa, come appunto volevasi dimostrare.

Giova forse osservare che in questo caso la verifica per $\boldsymbol{\sigma}^*$ appare sotto certi aspetti superflua. Infatti $\mathscr{S} = \mathscr{S}_{n_2}\mathscr{S}_{n_1}$ è una trasformazione ortogonale, quindi

$$B(\mathscr{S}\boldsymbol{\sigma},\ \mathscr{S}\boldsymbol{\sigma}^*) = 1, \qquad Q(\mathscr{S}\boldsymbol{\sigma}^*) = 0\,,$$

e da queste segue necessariamente che, poichè $\mathscr{S}\boldsymbol{\sigma} = p\,\boldsymbol{\sigma}$, deve essere

$$\mathscr{S}\boldsymbol{\sigma}^* = p^{-1}\,\boldsymbol{\sigma}^* .$$

Infine si aggiunga che la proprietà del nucleo delle trasformazioni ortogonali di essere sempre vuoto ha permesso di dedurre dalla ipotesi iniziale $\boldsymbol{\sigma} \notin U$ il fatto che $k \neq 0$, $k + 1 \neq 0$: queste conclusioni equivalgono ovviamente all'affermazione

$$\boldsymbol{\sigma} \notin U \Longrightarrow K \neq GF(2).$$

Caso B) $\boldsymbol{\sigma} \in U$.

Poichè $S^0 \supset U$, $U^0 \supset S$, e quindi $\boldsymbol{\sigma} \in U^0$ per cui

$$U \cap U^0 \neq \{0\},$$

cioè lo spazio U è necessariamente isotropo. A seconda che U sia solamente isotropo o totalmente isotropo, converrà distinguere nella dimostrazione due sottocasi.

Caso B_1) $\boldsymbol{\sigma} \in U$, $U^0 \notin U$.
Poichè U^0 ha dimensione 2 ed $U^0 \notin U$,

$$\dim_K (U \cap U^0) = 1 ,$$

per cui

$$U \cap U^0 = K\boldsymbol{\sigma} ,$$

e, passando agli spazi ortogonali,

$$U + U^0 = (K\boldsymbol{\sigma})^0 = S^0 = U \oplus K\boldsymbol{\omega} .$$

Ogni elemento di U^0 potrà dunque scriversi

$$\boldsymbol{u}^0 = \boldsymbol{u} + a\,\boldsymbol{\omega} ,$$

ove $\boldsymbol{u}$ indica un opportuno elemento di U ed a un opportuno elemento di K. Un qualsiasi elemento $\boldsymbol{u}^0$ siffatto gode di tutte le proprietà di $\boldsymbol{\omega}$: invero basterà prendere $a \neq 0$ perchè si abbia $\boldsymbol{u}^0 \notin U$, e siccome $\boldsymbol{\sigma} \in U$, segue immediata-

mente che

$$\boldsymbol{u}^0 + \boldsymbol{\sigma} \notin U .$$

Infine

$$\mathscr{P}\boldsymbol{u}^0 = \mathscr{P}\boldsymbol{u} + a\,\mathscr{P}\boldsymbol{\omega} = \boldsymbol{u} + a\,(\boldsymbol{\omega} + \boldsymbol{\sigma}) = \boldsymbol{u} + a\,\boldsymbol{\omega} + a\,\boldsymbol{\sigma} ,$$

quindi

$$\mathscr{P}\,\frac{\boldsymbol{u}^0}{a} = \frac{u + a\,\boldsymbol{\omega}}{a} + \boldsymbol{\sigma} = \frac{\boldsymbol{u}^0}{a} + \boldsymbol{\sigma} ,$$

cioè $\boldsymbol{u}^0/a$ può essere preso in sostituzione del vettore $\boldsymbol{\omega}$ iniziale o, conclusione equivalente alla precedente, si può supporre $\boldsymbol{\omega} \in U^0$, per cui

$$U^0 = K\boldsymbol{\sigma} \oplus K\boldsymbol{\omega} .$$

Il vettore $\boldsymbol{\omega}$ non può essere isotropo. Qualora lo fosse, si avrebbe

$$\boldsymbol{\omega} \in (K\boldsymbol{\omega})^0,$$

e siccome

$$U = (K\boldsymbol{\sigma} \oplus K\boldsymbol{\omega})^0 = (K\boldsymbol{\sigma})^0 \cap (K\boldsymbol{\omega})^0 = S^0 \cap (K\boldsymbol{\omega})^0$$

$$= (U \oplus K\boldsymbol{\omega}) \cap (K\boldsymbol{\omega})^0$$

si dovrebbe concludere che $\boldsymbol{\omega}$ appartiene ad U, contrariamente alle ipotesi. $\boldsymbol{\omega}$ è dunque un vettore non isotropo, cioè

$$B(\boldsymbol{\omega},\ \boldsymbol{\omega}) = 2\,Q(\boldsymbol{\omega}) \neq 0 ,$$

e quindi necessariamente nel sottocaso preso ora in esame *il corpo K ha caratteristica diversa da 2.*

Si può ora scegliere un vettore singolare $\boldsymbol{\sigma}^*$ tale che si abbia

$$B(\boldsymbol{\sigma},\ \boldsymbol{\sigma}^*) = 1;$$

ne segue che $\boldsymbol{\sigma}^* \notin S^0$ e quindi lo spazio iniziale V si decompone nella maniera seguente:

$$V = U \oplus K\boldsymbol{\omega} \oplus K\boldsymbol{\sigma}^*.$$

Si consideri ora lo spazio

$$U^* = U \cap (K\boldsymbol{\sigma}^*)^0:$$

poichè $\boldsymbol{\sigma} \notin (K\boldsymbol{\sigma}^*)^0$, $\boldsymbol{\sigma} \notin U^*$ e dunque $U = U^* \oplus K\boldsymbol{\sigma}$ per cui

$$V = U^* \oplus K\boldsymbol{\sigma} \oplus K\boldsymbol{\omega} \oplus K\boldsymbol{\sigma}^*.$$

Inoltre

$$U^{*0} = [U \cap (K\boldsymbol{\sigma}^*)^0]^0 = U^0 + K\boldsymbol{\sigma}^* = K\boldsymbol{\sigma} \oplus K\boldsymbol{\omega} \oplus K\boldsymbol{\sigma}^*.$$

Si consideri ora la pseudo-simmetria $\mathscr{P}_{\boldsymbol{\sigma},U,\boldsymbol{\omega}}$: poichè $U^* \subset U$,

$$\mathscr{P}\boldsymbol{u} = \boldsymbol{u} \qquad \text{per } \forall \boldsymbol{u} \in U^*;$$

poichè per ipotesi $\boldsymbol{\sigma} \in U$,

$$\mathscr{P}\boldsymbol{\sigma} = \boldsymbol{\sigma};$$

per definizione poi

$$\mathscr{P}\boldsymbol{\omega} = \boldsymbol{\omega} + \boldsymbol{\sigma}.$$

Rimane quindi da chiarire come opera la pseudo-simmetria $\mathscr{P}_{\boldsymbol{\sigma},U,\boldsymbol{\omega}}$ su $\boldsymbol{\sigma}^*$: si osservi intanto che essendo $\mathscr{P}U^* = U^*$, si ha

$$\mathscr{P}U^{*0} = U^{*0},$$

quindi

$$\mathscr{P}\boldsymbol{\sigma}^* = a\,\boldsymbol{\sigma} + b\,\boldsymbol{\omega} + c\,\boldsymbol{\sigma}^*, \qquad a,\ b,\ c \in K.$$

Inoltre, accanto alle

$$B(\boldsymbol{\sigma},\ \boldsymbol{\sigma}^*) = 1, \quad B(\boldsymbol{\sigma},\ \boldsymbol{\omega}) = 0, \quad Q(\boldsymbol{\sigma}) = 0, \quad Q(\boldsymbol{\sigma}^*) = 0,$$

si può sempre supporre

$$B(\boldsymbol{\omega},\ \boldsymbol{\sigma}^*) = 0.$$

Qualora fosse $B(\boldsymbol{\omega}, \boldsymbol{\sigma}^*) \neq 0$, si potrebbe porre

$$\boldsymbol{\omega}_1 = \boldsymbol{\omega} + m\,\boldsymbol{\sigma}\,, \qquad\qquad m \in K,\ m \neq 0:$$

si ha intanto $B(\boldsymbol{\omega}_1, \boldsymbol{\sigma}) = 0$ e basterebbe prendere $m = -B(\boldsymbol{\omega}, \boldsymbol{\sigma}^*)$ per avere in più $B(\boldsymbol{\omega}_1, \boldsymbol{\sigma}^*) = 0$, che è appunto la relazione richiesta. Il vettore $\boldsymbol{\omega}_1$ gode ancora di tutte le proprietà di cui gode $\boldsymbol{\omega}$: siccome $\boldsymbol{\omega} \notin U$ e $\boldsymbol{\sigma} \in U$, anche $\boldsymbol{\omega}_1 \notin U$, $\boldsymbol{\omega}_1 + \boldsymbol{\sigma} \notin U$ e

$$\mathscr{P}\boldsymbol{\omega}_1 = \mathscr{P}\boldsymbol{\omega} + \mathscr{P}\boldsymbol{\sigma} = \boldsymbol{\omega} + \boldsymbol{\sigma} + m\,\boldsymbol{\sigma} = \boldsymbol{\omega}_1 + \boldsymbol{\sigma}\,.$$

Si può dunque utilizzare il vettore $\boldsymbol{\omega}_1$ invece del vettore $\boldsymbol{\omega}$ introdotto nella definizione della pseudo-simmetria senza perciò modificare la $\mathscr{P}_{\sigma,U,\omega}$.

Allora

$$B(\mathscr{P}\boldsymbol{\sigma},\ \mathscr{P}\boldsymbol{\sigma}^*) = B(\boldsymbol{\sigma},\ a\,\boldsymbol{\sigma} + b\,\boldsymbol{\omega} + c\,\boldsymbol{\sigma}^*) = c = 1,$$

$$B(\mathscr{P}\boldsymbol{\omega},\ \mathscr{P}\boldsymbol{\sigma}^*) = B(\boldsymbol{\omega} + \boldsymbol{\sigma},\ a\,\boldsymbol{\sigma} + b\,\boldsymbol{\omega} + \boldsymbol{\sigma}^*) = 2b\,Q(\boldsymbol{\omega}) + 1 = 0,$$

quindi

$$b = -(1/2)\,Q^{-1}(\boldsymbol{\omega}),$$

$$Q(\mathscr{P}\boldsymbol{\sigma}^*) = Q\left(a\,\boldsymbol{\sigma} - \frac{1}{2}\,Q^{-1}(\boldsymbol{\omega})\,\boldsymbol{\omega} + \boldsymbol{\sigma}^*\right) = \frac{1}{4}\,Q^{-2}(\boldsymbol{\omega})\,Q(\boldsymbol{\omega}) + a = 0,$$

quindi

$$a = -(1/4)\,Q^{-1}(\boldsymbol{\omega})\,,$$

e dunque

$$\mathscr{P}\boldsymbol{\sigma}^* = \boldsymbol{\sigma}^* - (1/2)\,Q^{-1}(\boldsymbol{\omega})\,\boldsymbol{\omega} - (1/4)\,Q^{-1}(\boldsymbol{\omega})\,\boldsymbol{\sigma}\,.$$

I vettori

$$\boldsymbol{n}_1 = -(1/2)\,Q^{-1}(\boldsymbol{\omega})\,\boldsymbol{\omega} - (1/4)\,Q^{-1}(\boldsymbol{\omega})\,\boldsymbol{\sigma}, \qquad\qquad \boldsymbol{n}_2 = \boldsymbol{\omega} + \boldsymbol{\sigma}$$

sono non singolari, poichè

$$Q(\boldsymbol{n}_1) = Q[-(1/2)\,Q^{-1}(\boldsymbol{\omega})\,\boldsymbol{\omega} - (1/4)\,Q^{-1}(\boldsymbol{\omega})\,\boldsymbol{\sigma}] = (1/4)\,Q^{-2}(\boldsymbol{\omega})Q\,(\boldsymbol{\omega}) = (1/4)\,Q^{-1}(\boldsymbol{\omega}),$$

$$Q(\boldsymbol{n}_2) = Q(\boldsymbol{\omega} + \boldsymbol{\sigma}) = Q(\boldsymbol{\omega})\,.$$

Conseguentemente i vettori $\boldsymbol{n}_1$ ed $\boldsymbol{n}_2$ possono essere utilizzati per definire simmetrie. Inoltre questi due vettori sono elementi di U^{*0}, cioè sia $\boldsymbol{n}_1$ che $\boldsymbol{n}_2$

sono ortogonali ad U^*, per cui le simmetrie definite mediante questi vettori lasciano fissi tutti gli elementi di U^*, sicchè si può senz'altro scrivere

$$\mathscr{S}_{n_2}\mathscr{S}_{n_1}\boldsymbol{u} = \boldsymbol{u} \qquad \text{per } \forall \boldsymbol{u} \in U .$$

$\boldsymbol{n}_1$ ed $\boldsymbol{n}_2$ snoo pure ortogonali al vettore $\boldsymbol{\sigma}$ e quindi si ha ancora

$$\mathscr{S}_{n_2}\mathscr{S}_{n_1}\boldsymbol{\sigma} = \boldsymbol{\sigma} .$$

Si ha poi

$$\begin{aligned} \mathrm{S}_{n_1}\boldsymbol{\omega} &= \boldsymbol{\omega} - Q^{-1}(\boldsymbol{n}_1)\, B(\boldsymbol{n}_1,\ \boldsymbol{\omega})\boldsymbol{n}_1 \\ &= \boldsymbol{\omega} - 4\, Q(\boldsymbol{\omega})\, B[-(1/2)\, Q^{-1}(\boldsymbol{\omega})\, \boldsymbol{\omega} - (1/4)\, Q^{-1}(\boldsymbol{\omega})\, \boldsymbol{\sigma},\ \boldsymbol{\omega}]\, \boldsymbol{n}_1 \\ &= \boldsymbol{\omega} + 4\, Q(\boldsymbol{\omega})[-(1/2)\, Q^{-1}(\boldsymbol{\omega})\, \boldsymbol{\omega} - (1/4)\, Q^{-1}(\boldsymbol{\omega})\, \boldsymbol{\sigma}] \\ &= -\boldsymbol{\omega} - \boldsymbol{\sigma} = -\boldsymbol{n}_2 \end{aligned}$$

e quindi, per la terza proprietà delle simmetrie segnalata in precedenza,

$$\mathscr{S}_{n_2}\mathscr{S}_{n_1}\boldsymbol{\omega} = \mathscr{S}_{n_2}(-\boldsymbol{n}_2) = \boldsymbol{n}_2 = \boldsymbol{\omega} + \boldsymbol{\sigma} .$$

Infine

$$\begin{aligned} \mathscr{S}_{n_1}\boldsymbol{\sigma}^* &= \boldsymbol{\sigma}^* - Q^{-1}(\boldsymbol{n}_1)\, B(\boldsymbol{n}_1,\ \boldsymbol{\sigma}^*)\, \boldsymbol{n}_1 \\ &= \boldsymbol{\sigma}^* - 4\, Q(\boldsymbol{\omega})\, B[-(1/2)\, Q^{-1}(\boldsymbol{\omega})\, \boldsymbol{\omega} - (1/4)\, Q^{-1}(\boldsymbol{\omega})\, \boldsymbol{\sigma},\ \boldsymbol{\sigma}]\, \boldsymbol{n}_1 = \boldsymbol{\sigma}^* + \boldsymbol{n}_1, \\ \mathscr{S}_{n_2}\mathscr{S}_{n_1}\boldsymbol{\sigma}^* &= \boldsymbol{\sigma}^* + \boldsymbol{n}_1 - Q^{-1}(\boldsymbol{n}_2)\, B(\boldsymbol{\sigma}^* + \boldsymbol{n}_1,\ \boldsymbol{n}_2)\, \boldsymbol{n}_2 \\ &= \boldsymbol{\sigma}^* + \boldsymbol{n}_1 - Q^{-1}(\boldsymbol{\omega})\, \boldsymbol{n}_2 + Q^{-1}(\boldsymbol{\omega})\, \boldsymbol{n}_2 = \boldsymbol{\sigma}^* + \boldsymbol{n}_1 . \end{aligned}$$

Il prodotto delle simmetrie $\mathscr{S}_{n_1}$ ed $\mathscr{S}_{n_2}$ opera quindi esattamente come la pseudo-simmetria $\mathscr{P}_{\sigma,U,\omega}$ cioè coincide con essa, come appunto dovevasi dimostrare.

Caso B_2) $\boldsymbol{\sigma} \in U$, $U^0 \subset U$.

Dalla seconda delle relazioni scritte sopra segue che U^0 è uno spazio totalmente isotropo di dimensione 2, essendo infatti

$$(U^0)^0 \supset U^0 .$$

Per quanto è stato dimostrato riguardo alla decomposizione di WITT esiste dunque in V uno spazio U^*, di dimensione 2, totalmente isotropo, tale che U^0 ed U^* abbiano in comune soltanto il vettore nullo e che la somma diretta $U^0 \oplus U^*$ sia non isotropa. Poichè $\boldsymbol{\sigma}$ è singolare $B(\boldsymbol{\sigma}, \boldsymbol{\sigma}) = 0$ e quindi $\boldsymbol{\sigma} \in U^0$. Esiste dunque in U^0 un vettore $\boldsymbol{\rho}$ tale che

$$B(\boldsymbol{\rho}, \boldsymbol{\rho}) = 0, \qquad B(\boldsymbol{\rho}, \boldsymbol{\sigma}) = 0 ,$$

$$U^0 = K\boldsymbol{\rho} \oplus K\boldsymbol{\sigma} .$$

Sempre per la decomposizione di WITT, U^* deve contenere una base $\boldsymbol{\rho}^*$, $\boldsymbol{\sigma}^*$ concatenata alla base $\boldsymbol{\rho}$, $\boldsymbol{\sigma}$ di U^0, cioè esistono $\boldsymbol{\rho}^*$, $\boldsymbol{\sigma}^*$ tali che

$$Q(\boldsymbol{\sigma}^*) = 0, \quad B(\boldsymbol{\rho}^*, \boldsymbol{\rho}^*) = 0, \quad B(\boldsymbol{\rho}^*, \boldsymbol{\sigma}^*) = 0, \quad B(\boldsymbol{\rho}, \boldsymbol{\rho}^*) = 1,$$

$$B(\boldsymbol{\sigma}, \boldsymbol{\sigma}^*) = 1, \quad B(\boldsymbol{\rho}, \boldsymbol{\sigma}^*) = 0, \quad B(\boldsymbol{\sigma}, \boldsymbol{\rho}^*) = 0 ,$$

e che sia

$$U^* = K\boldsymbol{\rho}^* \oplus K\boldsymbol{\sigma}^* .$$

Infine si ha

$$V = U^0 \oplus U^* \oplus (U^0 \oplus U^*)^0 .$$

Orbene

$$(U^0 \oplus U^*)^0 = (U^0)^0 \cap U^{*0} \subset U ,$$

$$\dim_K (U^0 \oplus U^*)^0 = \dim_K V - 4 , \qquad \dim_K U = \dim_K V - 2 ,$$

quindi

$$U = U^0 \oplus (U^0 \oplus U^*)^0 .$$

Poichè U^* ha in comune con U soltanto il vettore nullo, U^* contiene la totalità dei vettori di V non contenuti in U, e quindi contiene pure $\boldsymbol{\omega}$. Si ha quindi

$$\boldsymbol{\omega} = a\,\boldsymbol{\rho}^* + b\,\boldsymbol{\sigma}^*, \qquad a, b \in K,$$

e poichè $\boldsymbol{\omega}$ deve appartenere ad $S^0 = (K\boldsymbol{\sigma})^0$, si ha $B(\boldsymbol{\omega}, \boldsymbol{\sigma}) = 0$, cioè

$$\boldsymbol{\omega} = a\,\boldsymbol{\rho}^*, \qquad a \in K,\ a \neq 0 .$$

È quindi senz'altro lecito prendere $\boldsymbol{\omega} = \boldsymbol{\rho}^*$ a condizione di sostituire in U^0 al vettore $\boldsymbol{\rho}$ della base concatenata il suo multiplo per a.

La pseudo-simmetria $\mathscr{P}_{\sigma,U,\omega} = \mathscr{P}$ inizialmente scelta opera in questo caso nella maniera seguente:

$$\mathscr{P}\boldsymbol{u} = \boldsymbol{u}, \qquad \text{per } \forall\, \boldsymbol{u} \in (U^0 \oplus U^*)^0,$$

$$\mathscr{P}\boldsymbol{\rho} = \boldsymbol{\rho}, \qquad \mathscr{P}\boldsymbol{\sigma} = \boldsymbol{\sigma},$$

perchè $\mathscr{P}$ per definizione lascia fissi tutti gli elementi appartenneti ad U:

$$\mathscr{P}\boldsymbol{\rho}^* = \boldsymbol{\rho}^* + \boldsymbol{\sigma},$$

perchè $\mathscr{P}$ applica $\boldsymbol{\omega}$ in $\boldsymbol{\omega} + \boldsymbol{\sigma}$; infine, poichè $\mathscr{P}$ lascia fisso ciascun vettore di $(U^0 \oplus U^*)^0$, si avrà

$$\mathscr{P}(U^0 \oplus U^*) = U^0 \oplus U^*,$$

cioè

$$\mathscr{P}\boldsymbol{\sigma}^* = a\,\boldsymbol{\rho} + b\,\boldsymbol{\sigma} + c\,\boldsymbol{\rho}^* + d\,\boldsymbol{\sigma}^*, \qquad a,\ b,\ c,\ d \in K.$$

Orbene

$$B(\mathscr{P}\boldsymbol{\sigma},\ \mathscr{P}\boldsymbol{\sigma}^*) = B(\boldsymbol{\sigma},\ \boldsymbol{\sigma}^*) = 1 \quad \Longrightarrow \quad d = 1,$$

$$B(\mathscr{P}\boldsymbol{\rho},\ \mathscr{P}\boldsymbol{\sigma}^*) = B(\boldsymbol{\rho},\ \boldsymbol{\sigma}^*) = 0 \quad \Longrightarrow \quad c = 0,$$

$$B(\mathscr{P}\boldsymbol{\rho}^*,\ \mathscr{P}\boldsymbol{\sigma}^*) = B(\boldsymbol{\rho}^*,\ \boldsymbol{\sigma}^*) = 0 \quad \Longrightarrow \quad a = -1,$$

$$Q(\mathscr{P}\boldsymbol{\sigma}^*) = Q(\boldsymbol{\sigma}^*) = 0 \quad \Longrightarrow \quad b = -Q(\boldsymbol{\rho}),$$

quindi

$$\mathscr{P}\boldsymbol{\sigma}^* = \boldsymbol{\sigma}^* - \boldsymbol{\rho} - Q(\boldsymbol{\rho})\,\boldsymbol{\sigma}.$$

Conviene ora procedere ad una ulteriore distinzione:

1°) *Il vettore* $\boldsymbol{\rho}$ *non è singolare.* Poichè $\boldsymbol{\rho}$ è isotropo si ha in tal caso

$$B(\boldsymbol{\rho},\ \boldsymbol{\rho}) = 2\,Q(\boldsymbol{\rho}) = 0 \qquad \text{con } Q(\boldsymbol{\rho}) \neq 0,$$

quindi necessariamente *il campo* K *ha caratteristica* 2.

Si considerino ora i vettori

$$\boldsymbol{n}_1 = Q(\boldsymbol{\rho})\,\boldsymbol{\sigma} + \boldsymbol{\rho}, \qquad \boldsymbol{n}_2 = \boldsymbol{\rho};$$

anzitutto

$$Q(\boldsymbol{n}_1) = Q^2(\boldsymbol{\rho})\,Q(\boldsymbol{\sigma}) + Q(\boldsymbol{\rho}) + Q(\boldsymbol{\rho})\,B(\boldsymbol{\sigma},\ \boldsymbol{\rho}) = Q(\boldsymbol{\rho}) \neq 0\,,$$

$$Q(\boldsymbol{n}_2) = Q(\boldsymbol{\rho}) \neq 0,$$

cioè i vettori $\boldsymbol{n}_1$ ed $\boldsymbol{n}_2$ sono non singolari. Inoltre $\boldsymbol{n}_1$ ed $\boldsymbol{n}_2$ appartengono ad U^0, cioè sono ortogonali ad U e dunque

$$\mathscr{S}_{n_2}\mathscr{S}_{n_1}\,\boldsymbol{u} = \boldsymbol{u} \qquad \text{per } \forall \boldsymbol{u} \in (U^0 \oplus U^*)^0,$$

$$\mathscr{S}_{n_2}\mathscr{S}_{n_1}\,\boldsymbol{\rho} = \boldsymbol{\rho}, \quad \mathscr{S}_{n_2}\mathscr{S}_{n_1}\,\boldsymbol{\sigma} = \boldsymbol{\sigma}.$$

Inoltre

$$\begin{aligned}\mathscr{S}_{n_1}\,\boldsymbol{\rho}^* &= \boldsymbol{\rho}^* - Q^{-1}(\boldsymbol{n}_1)\,B(\boldsymbol{n}_1,\ \boldsymbol{\rho}^*)\,\boldsymbol{n}_1 \\ &= \boldsymbol{\rho}^* - Q^{-1}(\boldsymbol{\rho})\,B[Q(\boldsymbol{\rho})\,\boldsymbol{\sigma} + \boldsymbol{\rho},\ \boldsymbol{\rho}^*]\,\boldsymbol{n}_1 = \boldsymbol{\rho}^* - Q^{-1}(\boldsymbol{\rho})\,\boldsymbol{n}_1,\end{aligned}$$

$$\begin{aligned}\mathscr{S}_{n_2}\mathscr{S}_{n_1}\,\boldsymbol{\rho}^* &= \boldsymbol{\rho}^* - Q^{-1}(\boldsymbol{\rho})\,\boldsymbol{n}_1 - Q^{-1}(\boldsymbol{n}_2)\,B[\boldsymbol{n}_2,\ \boldsymbol{\rho}^* - Q^{-1}(\boldsymbol{\rho})\,\boldsymbol{n}_1]\,\boldsymbol{n}_2 \\ &= \boldsymbol{\rho}^* - Q^{-1}(\boldsymbol{\rho})\,\boldsymbol{n}_1 - Q^{-1}(\boldsymbol{\rho})\,\boldsymbol{n}_2 = \boldsymbol{\rho}^* - Q^{-1}(\boldsymbol{\rho})\,Q(\boldsymbol{\rho})\,\boldsymbol{\sigma} \\ &= \boldsymbol{\rho}^* - \boldsymbol{\sigma} = \boldsymbol{\rho}^* + \boldsymbol{\sigma}\,.\end{aligned}$$

Infine

$$\begin{aligned}\mathscr{S}_{n_1}\,\boldsymbol{\sigma}^* &= \boldsymbol{\sigma}^* - Q^{-1}(\boldsymbol{n}_1)\,B(\boldsymbol{n}_1,\ \boldsymbol{\sigma}^*)\,\boldsymbol{n}_1 = \boldsymbol{\sigma}^* - Q^{-1}(\boldsymbol{\rho})\,Q(\boldsymbol{\rho})\,\boldsymbol{n}_1 \\ &= \boldsymbol{\sigma}^* - \boldsymbol{n}_1,\end{aligned}$$

$$\begin{aligned}\mathscr{S}_{n_2}\mathscr{S}_{n_1}\,\boldsymbol{\sigma}^* &= \boldsymbol{\sigma}^* - \boldsymbol{n}_1 - Q^{-1}(\boldsymbol{n}_2)\,B(\boldsymbol{n}_2,\ \boldsymbol{\sigma}^* - \boldsymbol{n}_1)\,\boldsymbol{n}_2 = \boldsymbol{\sigma}^* - \boldsymbol{n}_1 \\ &= \boldsymbol{\sigma}^* - Q(\boldsymbol{\rho})\,\boldsymbol{\sigma} - \boldsymbol{\rho}\,.\end{aligned}$$

Si ha quindi che il prodotto delle simmetrie rispetto ad $\boldsymbol{n}_1$ ed $\boldsymbol{n}_2$ opera come $\mathscr{P}$, cioè

$$\mathscr{S}_{n_2}\mathscr{S}_{n_1} \equiv \mathscr{P}\,.$$

2°) *Il vettore* ρ *è singolare.* In questo caso U^0 è totalmente singolare e quindi anche U^* sarà totalmente singolare, per cui

$$Q(\rho) = 0, \qquad Q(\rho^*) = 0 .$$

Si deve allora procedere ad una nuova distinzione in due casi, a seconda della natura del campo K.

2°)′ Il campo K ha più di due elementi, cioè $K \neq GF(2)$. Indicato con m un elemento di K distinto da 0 ed 1, i vettori

$$\boldsymbol{n}_1 = \rho + \frac{m}{1-m}\sigma + m\,\rho^*, \qquad \boldsymbol{n}_2 = \rho + \frac{1}{1-m}\sigma + \rho^*,$$

$$\boldsymbol{n}_3 = \rho + \sigma + \rho^*, \qquad \boldsymbol{n}_4 = \rho + m(\sigma + \rho^*)$$

sono tutti non singolari, essendo

$$Q(\boldsymbol{n}_1) = Q(\boldsymbol{n}_4) = m \neq 0, \qquad Q(\boldsymbol{n}_2) = Q(\boldsymbol{n}_3) = 1 \neq 0 .$$

Inoltre questi vettori sono ortogonali ad ogni $\boldsymbol{u} \in (U^0 \oplus U^*)^0$ ed a σ, quindi

$$\mathcal{S}_{n_i}\boldsymbol{u} = \boldsymbol{u}, \qquad \mathcal{S}_{n_i}\sigma = \sigma \qquad \text{per } \forall \boldsymbol{u} \in (U^0 \oplus U^*)^0,\ i \in (1,4),$$

$$\mathcal{S}_{n_4}\mathcal{S}_{n_3}\mathcal{S}_{n_2}\mathcal{S}_{n_1}\boldsymbol{u} = \boldsymbol{u} \qquad \text{per } \forall \boldsymbol{u} \in (U^0 \oplus U^*)^0,$$

$$\mathcal{S}_{n_4}\mathcal{S}_{n_3}\mathcal{S}_{n_2}\mathcal{S}_{n_1}\sigma = \sigma .$$

Inoltre

$$\mathcal{S}_{n_1}\rho^* = -(1/m)\,\rho - \frac{1}{1-m}\sigma,$$

$$\mathcal{S}_{n_2}\mathcal{S}_{n_1}\rho^* = (1/m)(\rho^* + \sigma),$$

$$\mathcal{S}_{n_3}\mathcal{S}_{n_2}\mathcal{S}_{n_1}\rho^* = -(1/m)\,\rho,$$

$$\mathcal{S}_{n_4}\mathcal{S}_{n_3}\mathcal{S}_{n_2}\mathcal{S}_{n_1}\rho^* = \rho^* + \sigma,$$

$$\mathcal{S}_{n_1}\rho = -\frac{m}{1-m}\sigma - m\rho^*,$$

$$\mathcal{S}_{n_2}\mathcal{S}_{n_1}\rho = m\,\rho,$$

$$\mathcal{S}_{n_3}\mathcal{S}_{n_2}\mathcal{S}_{n_1}\rho = -m\,(\sigma + \rho^*),$$

$$\mathcal{S}_{n_4}\mathcal{S}_{n_3}\mathcal{S}_{n_2}\mathcal{S}_{n_1}\rho = \rho,$$

ed infine

$$\mathscr{S}_{n_1}\sigma^* = -\frac{1}{1-m}\rho - \frac{1}{1-m}\frac{m}{1-m}\sigma - \frac{m}{1-m}\rho^* + \sigma^*,$$

$$\mathscr{S}_{n_2}\mathscr{S}_{n_1}\sigma^* = \sigma^* - \rho\,.$$

Siccome $\boldsymbol{n}_3$ ed $\boldsymbol{n}_4$ sono ambedue ortogonali a $\sigma^* - \rho$, se ne deduce immediatamente che

$$\mathscr{S}_{n_4}\mathscr{S}_{n_3}\mathscr{S}_{n_2}\mathscr{S}_{n_1}\sigma^* = \sigma^* - \rho,$$

e così risulta dimostrato che il prodotto delle simmetrie definite mediante i quattro vettori non singolari $\boldsymbol{n}_i$ ($i \in (1, 4)$) coincide ovunque su V con la pseudosimmetria $\mathscr{P}$.

2°)" Evidentemente i vettori $\boldsymbol{n}_i$ introdotti in precedenza non possono essere definiti se $K = GF(2)$. In tal caso si supponga lo spazio $(U^0 \oplus U^*)^0$ non vuoto: per quanto si è visto sulla decomposizione di WITT, esiste allora in questo spazio un vettore non singolare $\boldsymbol{a}$. Siccome K ha caratteristica 2 ed è costituito dai soli elementi 0 ed 1, deve dunque essere $Q(\boldsymbol{a}) = 1$. I vettori

$$\boldsymbol{n}_1 = \rho + \boldsymbol{a}, \qquad \boldsymbol{n}_2 = \sigma + \boldsymbol{a}, \qquad \boldsymbol{n}_3 = \boldsymbol{a}, \qquad \boldsymbol{n}_4 = \rho + \sigma + \boldsymbol{a}$$

sono allora tutti non singolari, essendo

$$Q(\boldsymbol{n}_i) = Q(\boldsymbol{a}) = 1 \neq 0, \qquad i \in (1, 4).$$

Questi vettori essendo inoltre ortogonali sia a ρ che a σ si ha

$$\mathscr{S}_{n_i}\rho = \rho, \qquad \mathscr{S}_{n_i}\sigma = \sigma, \qquad i \in (1, 4)\,,$$

quindi

$$\mathscr{S}_{n_4}\mathscr{S}_{n_3}\mathscr{S}_{n_2}\mathscr{S}_{n_1}\rho = \rho, \qquad \mathscr{S}_{n_4}\mathscr{S}_{n_3}\mathscr{S}_{n_2}\mathscr{S}_{n_1}\sigma = \sigma\,.$$

Inoltre, tenendo presente che $K = GF(2)$, si ha

$$\mathscr{S}_{n_1}\rho^* = \rho^* + \rho + \boldsymbol{a};$$

$\boldsymbol{n}_2$ ed $\boldsymbol{n}_3$ sono ortogonali a $\rho + \rho^* + \boldsymbol{a}$, e quindi

$$\mathscr{S}_{n_3}\mathscr{S}_{n_2}\mathscr{S}_{n_1}\rho^* = \rho^* + \rho + \boldsymbol{a}\,,$$

e da qui infine

$$\mathcal{S}_{n_4}\mathcal{S}_{n_3}\mathcal{S}_{n_2}\mathcal{S}_{n_1}\rho^* = \rho^* + \rho + a + \rho + \sigma + a = \rho^* + \sigma .$$

Similmente

$$\mathcal{S}_{n_1}\sigma^* = \sigma ,$$

$$\mathcal{S}_{n_2}\mathcal{S}_{n_1}\sigma^* = \sigma^* + \sigma + a ,$$

$$\mathcal{S}_{n_3}\mathcal{S}_{n_2}\mathcal{S}_{n_1}\sigma^* = \sigma^* + \sigma + a ,$$

$$\mathcal{S}_{n_4}\mathcal{S}_{n_3}\mathcal{S}_{n_2}\mathcal{S}_{n_1}\sigma^* = \sigma^* + \rho .$$

Finalmente, per $\forall \boldsymbol{u} \in (U^0 \oplus U^*)^0$,

$$\mathcal{S}_{n_1}\boldsymbol{u} = B(\boldsymbol{a}, \boldsymbol{u})(\rho + \boldsymbol{a}) ,$$

$$\mathcal{S}_{n_2}\mathcal{S}_{n_1}\boldsymbol{u} = \boldsymbol{u} + B(\boldsymbol{a}, \boldsymbol{u})(\rho + \sigma) ,$$

$$\mathcal{S}_{n_3}\mathcal{S}_{n_2}\mathcal{S}_{n_1}\boldsymbol{u} = \boldsymbol{u} + B(\boldsymbol{a}, \boldsymbol{u})(\rho + \sigma + \boldsymbol{a}) ,$$

$$\mathcal{S}_{n_4}\mathcal{S}_{n_3}\mathcal{S}_{n_2}\mathcal{S}_{n_1}\boldsymbol{u} = \boldsymbol{u} ,$$

e dunque ancora

$$\mathcal{S}_{n_4}\mathcal{S}_{n_3}\mathcal{S}_{n_2}\mathcal{S}_{n_1} \equiv \mathcal{P} .$$

Evidentemente questa dimostrazione viene meno se $(U^0 \oplus U^*)^0$ è vuoto, cioè se $K = GF(2)$, $\dim_K V = 4$, $\dim_K U = 2$.

13. - Lo spazio eccezionale.

Per completare i risultati esposti sinora, è opportuno esaminare il caso rimasto escluso dalle precedenti due dimostrazioni e mostrare effettivamente che non rientra nel teorema generale.

Si consideri dunque lo spazio vettoriale V, con $\dim_K V = 4$, costruito su $K = GF(2)$ e tale che V contenga uno spazio totalmente singolare di dimensione 2. Se $(\boldsymbol{e}_1, \boldsymbol{e}_2)$ ed (ϵ_1, ϵ_2) sono basi nei due spazi totalmente singolari nei quali si decompone V, che siano concatenate, nel senso chiarito in precedenza, i 16 vettori che costituiscono tutto questo spazio potranno scriversi

$$0, \quad e_1, \quad e_2, \quad \epsilon_1, \quad \epsilon_2,$$

$$e_1 + \epsilon_2, \quad e_2 + \epsilon_1, \quad e_1 + e_2, \quad \epsilon_1 + \epsilon_2, \quad e_1 + e_2 + \epsilon_1 + \epsilon_2,$$

ed

$$n_1 = e_1 + \epsilon_1, \qquad n_2 = e_2 + \epsilon_2 + \epsilon_1, \qquad n_3 = e_2 + \epsilon_2 + e_1,$$
$$n_1' = e_2 + \epsilon_2, \qquad n_2' = e_1 + \epsilon_1 + \epsilon_2, \qquad n_3' = e_1 + \epsilon_1 + e_2;$$

i primi dieci sono tutti singolari mentre gli ultimi sei sono invece non singolari. I soli due sottospazi vettoriali di dimensione 2, cioè i due soli piani, *non singolari* di V, sono i piani P e P': il primo contiene, oltre il vettore nullo, i tre vettori non singolari n_1, n_2, n_3, mentre il secondo, oltre il vettore nullo, contiene i vettori non singolari n_1', n_2', n_3'. Date le proprietà delle trasformazioni ortogonali segnalate in precedenza, ogni elemento del gruppo ortogonale o trasforma V applicando questi spazi in sè stessi, oppure li permuta fra di loro.

Se ν denota uno qualsiasi dei vettori n_i o n_i', $i \in (1, 3)$, si ha evidentemente

$$B(\nu, \nu) = 2\, Q(\nu) = 0$$

perchè il campo K ha caratteristica 2, e quindi $\mathcal{S}_\nu \nu = \nu$; segue da ciò che le simmetrie definite mediante i vettori non singolari ν, e di conseguenza qualsiasi elemento appartenente al gruppo G' generato da queste simmetrie, opera in V trasformando in sè stessi sia il piano P che il piano P': il gruppo G' è quindi effettivamente contenuto nel gruppo G, senza con ciò venire a coincidere con esso.

Si ha invece

$$B(n_i, n_j) = 1, \quad B(n_i, n_j') = 0, \quad B(n_i', n_j') = 1, \qquad i, j \in (1, 3),\ i \neq j,$$

e quindi la simmetria definita, ad esempio, dal vettore non singolare n_i lascia fissi il vettore n_i stesso e tutti i vettori del piano a cui non appartiene ed al quale è ortogonale, cioè i vettori n_1', n_2', n_3'. Poichè questa simmetria non può essere l'identità, necessariamente opera permutando fra di loro i vettori n_j ed n_k ($i \neq j \neq k \neq i$, $i, j, k \in (1, 3)$). Le simmetrie $\mathcal{S}_{n_1}$, $\mathcal{S}_{n_2}$ ed $\mathcal{S}_{n_3}$ generano dunque una struttura isomorfa a quella generata dalle permutazioni

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

cioè generano una struttura isomorfa al gruppo delle permutazioni di tre elementi. Altrettanto si può dire della struttura generata dalle tre simmetrie

$\mathscr{S}_{n_i'}$, $i \in (1, 3)$, e quindi il gruppo G' è

$$G' = \mathscr{G}_3 \times \mathscr{G}_3 .$$

Invece la trasformazione ortogonale $\mathscr{T}$ definita mediante le condizioni

$$\mathscr{T}\boldsymbol{e}_1 = \boldsymbol{e}_2, \qquad \mathscr{T}\boldsymbol{e}_2 = \boldsymbol{e}_1, \qquad \mathscr{T}\boldsymbol{\epsilon}_1 = \boldsymbol{\epsilon}_2, \qquad \mathscr{T}\boldsymbol{\epsilon}_2 = \boldsymbol{\epsilon}_1,$$

opera sui vettori $\boldsymbol{n}_i$ ed $\boldsymbol{n}_i'$, scambiandoli fra di loro e quindi permuta fra di loro i piani P e P', cioè non appartiene a G' pur essendo contenuta in G. Si verifica facilmente che

$$G = \mathscr{T}G' \oplus G'.$$

Appendice.

Per definire le simmetrie necessarie per i successivi sviluppi sia della prima che della seconda dimostrazione del teorema di CARTAN e DIEUDONNÉ sono stati introdotti in vari momenti alcuni vettori non singolari, indicati ovunque con la scrittura $\boldsymbol{n}_i$ (cfr. pagine 190, 191, 192, 193, 205, 209, 210, 213, 214, 215). Le espressioni esplicite di questi vettori non sono sempre semplici ed il criterio che ha guidato la scelta non è sempre ovvio, per cui viene spontaneo chiedersi in qual maniera si sia proceduto per la determinazione di questi vettori.

La risposta a questo quesito va cercata nella proprietà fondamentale del Lemma A, proprietà che afferma che due vettori tali che la forma quadratica Q prenda per ambedue ugual valore sono applicati l'un nell'altro dalla simmetria definita dalla loro differenza, purchè questa risulti non singolare. Se ne conclude che se $\boldsymbol{s}$ è singolare ed $\boldsymbol{n}$ è non singolare

$$\boldsymbol{s} \xrightarrow[\mathscr{S}_n]{} \boldsymbol{n} - \boldsymbol{s} ,$$

purchè $\boldsymbol{n} - \boldsymbol{s}$ sia parimenti non singolare.

Il procedimento verrà chiarito in tutti i suoi particolari per la quaterna di vettori utilizzata a pagina 215.

Si considerino le proprietà della pseudo-simmetria utilizzata in quel caso; queste si riassumono nelle seguenti formule:

$$\mathscr{P}\boldsymbol{u} = \boldsymbol{u} \qquad \text{per } \forall \boldsymbol{u} \in (U^0 \oplus U^*)^0,$$

$$\mathscr{P}\boldsymbol{\rho} = \boldsymbol{\rho}, \qquad \mathscr{P}\boldsymbol{\sigma} = \boldsymbol{\sigma}, \qquad \mathscr{P}\boldsymbol{\rho}^* = \boldsymbol{\rho}^* + \boldsymbol{\sigma}, \qquad \mathscr{P}\boldsymbol{\sigma}^* = \boldsymbol{\sigma}^* - \boldsymbol{\rho} .$$

Scegliendo i vettori $\boldsymbol{n}_i$ nello spazio $U^0 \oplus U^*$ è evidente che la prima delle proprietà elencate sopra risulta immediatamente verificata da qualsiasi prodotto delle simmetrie definite mediante questi vettori. È quindi conveniente supporre

$$\boldsymbol{n}_i = a_i\,\boldsymbol{\rho} + b_i\,\boldsymbol{\sigma} + c_i\,\boldsymbol{\rho}^* + d_i\,\boldsymbol{\sigma}^*, \qquad a_i,\ b_i,\ c_i,\ d_i \in K, \quad i \in (1,\ 4).$$

Se parimenti si suppongono ortogonali a $\boldsymbol{\sigma}$ tutt'e quattro i vettori $\boldsymbol{n}_i$ si ha

$$\boldsymbol{\sigma} \xrightarrow[\mathscr{S}_{n_1}]{} \boldsymbol{\sigma} \xrightarrow[\mathscr{S}_{n_2}]{} \boldsymbol{\sigma} \xrightarrow[\mathscr{S}_{n_3}]{} \boldsymbol{\sigma} \xrightarrow[\mathscr{S}_{n_4}]{} \boldsymbol{\sigma},$$

per cui

$$\mathscr{S}_{n_4}\mathscr{S}_{n_3}\mathscr{S}_{n_2}\mathscr{S}_{n_1}\boldsymbol{\sigma} = \boldsymbol{\sigma}\,.$$

Deve quindi essere

$$B(\boldsymbol{n}_i,\ \boldsymbol{\sigma}) = 0, \qquad i \in (1,\ 4)\,,$$

cioè

$$d_i = 0\,, \qquad i \in (1,\ 4)\,.$$

Per determinare alcuni dei rimanenti 12 parametri arbitrari si potrà anzitutto supporre che $\boldsymbol{n}_1$ ed $\boldsymbol{n}_2$ siano tali che la coppia di simmetrie rispetto a questi vettori realizzi quanto è richiesto dalle condizioni del problema, e che le simmetrie rispetto ai rimanenti due vettori non cambino la situazione. Per questo, indicato con $\boldsymbol{s}$ un vettore singolare, basterà supporre

$$\text{(I)} \qquad h\,\boldsymbol{n}_1 = \boldsymbol{\sigma}^* - \boldsymbol{s}, \quad k\,\boldsymbol{n}_2 = \boldsymbol{s} - \boldsymbol{\sigma}^* + \boldsymbol{\rho}, \qquad h,\ k \in K,\ h \neq 0,\ k \neq 0,$$

e prendere $\boldsymbol{n}_3$ ed $\boldsymbol{n}_4$ ortogonali ad $\boldsymbol{\sigma}^* - \boldsymbol{\rho}$: si avrà allora

$$\boldsymbol{\sigma}^* \xrightarrow[\mathscr{S}_{n_1}]{} \boldsymbol{s} \xrightarrow[\mathscr{S}_{n_2}]{} \boldsymbol{\sigma}^* - \boldsymbol{\rho} \xrightarrow[\mathscr{S}_{n_3}]{} \boldsymbol{\sigma}^* - \boldsymbol{\rho} \xrightarrow[\mathscr{S}_{n_4}]{} \boldsymbol{\sigma}^* - \boldsymbol{\rho},$$

per cui ancora

$$\mathscr{S}_{n_4}\mathscr{S}_{n_3}\mathscr{S}_{n_2}\mathscr{S}_{n_1}\boldsymbol{\sigma}^* = \boldsymbol{\sigma}^* - \boldsymbol{\rho}\,.$$

Si verifica immediatamente che in tal caso devono essere soddisfatte le condizioni

$$\text{(II)} \quad h\,a_1\,c_1 - b_1 = 0, \qquad k\,a_2\,c_2 - c_2 + b_2 = 0, \qquad b_3 - c_2 = 0, \qquad b_4 - c_4 = 0\,.$$

Inoltre, eliminando il vettore singolare $\boldsymbol{s}$ dalle (I), si trova l'equazione vettoriale

$$h\,\boldsymbol{n}_1 + k\,\boldsymbol{n}_2 = \boldsymbol{\rho},$$

che fornisce ancora tre equazioni scalari, e precisamente

$$\text{(III)} \qquad h\,a_1 + k\,a_2 = 1, \qquad h\,b_1 + k\,b_2 = 0, \qquad h\,c_1 + k\,c_2 = 0\,.$$

Si verifica facilmente che il sistema formato riunendo (II) e (III) contiene soltanto sei equazioni indipendenti e quindi è possibile eliminare h, k e quattro dei dodici parametri che intervengono nella determinazione degli $\boldsymbol{n}_i$. Si ha

$$b_1 = \frac{a_1 c_1 c_2}{a_1 c_2 - a_2 c_1}\,, \qquad b_2 = \frac{a_1 c_2^2}{a_1 c_2 - a_2 c_1}\,, \qquad b_3 = c_3, \qquad b_4 = c_4\,,$$

$$h = \frac{c_2}{a_1 c_2 - a_2 c_1} \neq 0\,,$$

per cui

$$\boldsymbol{n}_1 = a_1\,\boldsymbol{\rho} + h\,a_1 c_1\,\boldsymbol{\sigma} + c_1\,\boldsymbol{\rho}^*, \qquad \boldsymbol{n}_2 = a_2\,\boldsymbol{\rho} + h\,a_1 c_2\,\boldsymbol{\sigma} + c_2\,\boldsymbol{\rho}^*,$$

$$\boldsymbol{n}_3 = a_3\,\boldsymbol{\rho} + c_3\,\boldsymbol{\sigma} + c_3\,\boldsymbol{\rho}^*, \qquad \boldsymbol{n}_4 = a_4\,\boldsymbol{\rho} + c_4\,\boldsymbol{\sigma} + c_4\,\boldsymbol{\rho}^*.$$

Il fatto che i vettori $\boldsymbol{n}_i$ devono essere non singolari impone inoltre ai parametri la condizione

$$a_i\,c_i \neq 0, \qquad \text{cioè} \qquad a_i \neq 0, \quad c_i \neq 0, \qquad\qquad i \in (1,\ 4)\,.$$

Perchè il prodotto delle simmetrie definite mediante i vettori $\boldsymbol{n}_i$, prese nell'ordine utilizzato sinora, goda delle rimanenti due proprietà della pseudo-simmetria $\mathscr{P}$ è necessario anzitutto che si abbia

$$\boldsymbol{\rho} \xrightarrow[\mathscr{S}_{n_1}]{} \boldsymbol{s}_{11} \xrightarrow[\mathscr{S}_{n_2}]{} \boldsymbol{s}_{12} \xrightarrow[\mathscr{S}_{n_3}]{} \boldsymbol{s}_{13} \xrightarrow[\mathscr{S}_{n_4}]{} \boldsymbol{\rho}\,.$$

ove i vettori $\boldsymbol{s}_{ij}$ $(j \in (1,\ 3))$ sono tutti singolari. Perchè la prima applicazione operi com'è stato indicato sopra deve essere, in base al Lemma A,

$$p_1\,\boldsymbol{n}_1 = \boldsymbol{\rho} - \boldsymbol{s}_{11}, \qquad\qquad p_1 \in K, \quad p_1 \neq 0\,,$$

e quindi

$$p_1 = a_1^{-1}, \qquad \boldsymbol{s}_{11} = -\,c_1\{\,h\,\boldsymbol{\sigma} + (1/a_1)\,\boldsymbol{\rho}^*\,\}.$$

Perchè la seconda applicazione operi secondo lo schema prescelto deve essere

$$p_2\,\boldsymbol{n}_2 = \boldsymbol{s}_{11} - \boldsymbol{s}_{12}, \qquad\qquad p_2 \in K, \quad p_2 \neq 0,$$

per cui

$$p_2 = -\frac{c_1}{a_1\, c_2}, \qquad \boldsymbol{s}_{12} = \frac{c_1\, a_2}{a_1\, c_2}\,\boldsymbol{\rho}\,.$$

Perchè la terza applicazione operi secondo lo schema prescelto deve essere

$$p_3\,\boldsymbol{n}_3 = \boldsymbol{s}_{12} - \boldsymbol{s}_{13}, \qquad p_3 \in K, \quad p_3 \neq 0\,,$$

per cui

$$p_3 = \frac{c_1\, a_2}{a_1\, c_2\, a_3}, \qquad \boldsymbol{s}_{13} = -\frac{c_1\, a_2\, c_3}{a_1\, c_2\, a_3}\,(\boldsymbol{\sigma} + \boldsymbol{\rho}^*)\,,$$

ed infine perchè la quarta applicazione operi secondo lo schema prescelto deve essere

$$p_4\,\boldsymbol{n}_4 = \boldsymbol{s}_{13} - \boldsymbol{\rho}\,, \qquad p_4 \in K, \quad p_4 \neq 0\,,$$

per cui

$$p_4 = \frac{1}{a_4} = \frac{c_1\, a_2\, c_3}{a_1\, c_2\, a_3\, c_4}, \qquad c_4 = \frac{c_1\, a_2\, c_3}{a_1\, c_2\, a_3}\,a_4\,.$$

Infine, perchè l'ultima delle proprietà di $\mathscr{P}$ sia realizzata dal prodotto deve essere

$$\boldsymbol{\rho}^* \xrightarrow[\mathscr{S}_{n_1}]{} \boldsymbol{s}_{21} \xrightarrow[\mathscr{S}_{n_2}]{} \boldsymbol{s}_{22} \xrightarrow[\mathscr{S}_{n_3}]{} \boldsymbol{s}_{23} \xrightarrow[\mathscr{S}_{n_4}]{} \boldsymbol{\rho}^* + \boldsymbol{\sigma},$$

i vettori $\boldsymbol{s}_{2j}$ $(j \in (1, 3))$ essendo ancora tutti vettori singolari. Perchè le quattro simmetrie considerate operino secondo lo schema dovrà essere:

a) $$q_1\,\boldsymbol{n}_1 = \boldsymbol{\rho}^* - \boldsymbol{s}_{21}, \qquad q_1 \in K,\ q_1 \neq 0\,,$$

quindi

$$q_1 = c_1^{-1}, \qquad \boldsymbol{s}_{21} = -\,a_1\{(1/c_1)\,\boldsymbol{\rho} + h\,\boldsymbol{\sigma}\};$$

b) $$q_2\,\boldsymbol{n}_2 = \boldsymbol{s}_{21} - \boldsymbol{s}_{22}, \qquad q_2 \in K,\ q_2 \neq 0\,,$$

quindi

$$q_2 = -\frac{a_1}{c_1\, a_2}, \qquad \boldsymbol{s}_{22} = h\, a_1\,\frac{a_1\, c_2 - c_1\, a_2}{a_2\, c_1}\,\boldsymbol{\sigma} + \frac{a_1\, c_2}{c_1\, a_2}\,\boldsymbol{\rho}^*,$$

ossia, sostituendo ad h il suo valore determinato sopra,

$$\boldsymbol{s}_{22} = \frac{a_1\, c_2}{a_2\, c_1}\,(\boldsymbol{\rho}^* + \boldsymbol{\sigma});$$

c) $$q_3\,\boldsymbol{n}_3 = \boldsymbol{s}_{22} - \boldsymbol{s}_{23}, \qquad q_3 \in K,\ q_3 \neq 0\,,$$

quindi

$$q_3 = \frac{a_1 c_2}{c_1 a_2 c_3}, \qquad s_{23} = -\frac{a_1 c_2 a_3}{c_1 a_2 c_3}\,\rho;$$

d) $$q_4 \boldsymbol{n}_4 = s_{23} - (\rho^* + \sigma), \qquad q_4 \in K, \quad q_4 \neq 0,$$

quindi

$$q_4 = -\frac{a_1 c_2 a_3}{c_1 a_2 c_3 a_4}.$$

Si conclude quindi che il sistema

(IV)
$$\begin{cases} \boldsymbol{n}_1 = a_1\,\rho + \dfrac{a_1 c_1 c_2}{a_1 c_2 - a_2 c_1}\,\sigma + c_1\rho^* \\ \boldsymbol{n}_2 = a_2\,\rho + \dfrac{a_1 c_2^2}{a_1 c_2 - a_2 c_1}\,\sigma + c_2\rho^* \\ \boldsymbol{n}_3 = a_3\,\rho + c_3\,\sigma + c_3\,\rho^* \\ \boldsymbol{n}_4 = a_4\,\rho + \dfrac{c_1 a_2 c_3 a_4}{a_1 c_2 a_3}\,\sigma + \dfrac{c_1 a_2 c_3 a_4}{a_1 c_2 a_3}\,\rho^*, \end{cases}$$

ove

$$a_i,\ c_i,\ a_1 c_2 - c_1 a_2 \neq 0, \qquad i \in (1,\ 4),$$

rappresenta la forma più generale che possano assumere i vettori $\boldsymbol{n}_i$. È evidente che se il campo K è costituito dai soli due elementi 0 ed 1, dovendo sia gli a_i che i c_i essere non nulli, tutti questi parametri dovranno essere uguali ad 1 ed i vettori $\boldsymbol{n}_1$ ed $\boldsymbol{n}_2$ non si potranno più definire, mentre $\boldsymbol{n}_3$ ed $\boldsymbol{n}_4$ coincidono. Se il campo K contiene tre elementi distinti 0, 1, ed m, il sistema (IV) si potrà, ad esempio, scrivere come a pagina 215.

Per la determinazione degli altri gruppi di vettori $\boldsymbol{n}_i$ utilizzati nelle pagine precedenti si è seguito sempre una procedura analoga.

Bibliografia.

[1] E. CARTAN, *Leçons sur la Théorie des Spineurs*, Actualités Sci. Industr. **643**, Hermann, Paris 1938.

[2] J. DIEUDONNÉ, *Sur les groupes classiques*, Actualités Sci. Industr. **1040**, Hermann, Paris 1948.

[3] E. WITT, *Theorie der quadratischen Formen in beliebigen Körpen*, J. de Crelle **176** (1937), 31-44.

[4] C. ARF, *Untersuchungen über quadratischen Formen in Körpern der Charakteristik* 2, J. de Crelle **183** (1941), 148-167.

[5] Dimostrazioni che non tengono conto del caso di K con caratteristica 2, e quindi non toccano il caso eccezionale:

a) N. BOURBAKI, *Formes sesquilinéaires et formes quadratiques* (Algébre 9), Actualités Sci. Industr. **1272**, Hermann, Paris 1959 (cfr. pp. 97-98).

b) O. T. O'MEARA, *Introduction to quadratic forms*, Springer, Berlin 1963 (cfr. pp. 102-103).

Dimostrazioni che tengono presente il caso dei campi a caratteristica 2:

a) J. DIEUDONNÉ, loc. cit. in [2].

b) C. C. CHEVALLEY, *The algebraic theory of spinors*, Columbia Univ. Press, NewYork 1954 (cfr. pp. 19-23).

* * *