Classification des formes quadratiques sur $\mathbb{F}_q$

Lemme Soit $\mathbb{F}_q$ un corps de caractéristique différente de 2.
L'équation en x, y : $ax^2 + by^2 = 1$ avec $a, b \in \mathbb{F}_q^*$ admet des solutions dans $\mathbb{F}_q$.

On considère le morphisme :
$\varphi : \mathbb{F}_q^* \longrightarrow \mathbb{F}_q^{*2}, \ x \longmapsto x^2$
On a alors :
$\operatorname{Ker} \varphi = \{-1, 1\}$
Donc par le 1er théorème d'isomorphisme et égalité des cardinaux :
$$|\mathbb{F}_q^{*2}| = \frac{|\mathbb{F}_q^*|}{2} = \frac{q-1}{2}$$

De plus, $0 \in \mathbb{F}_q^2$ donc $|\mathbb{F}_q^2| = |\mathbb{F}_q^{*2}| + 1 = \frac{q+1}{2}$.

Alors :
lorsque y parcourt $\mathbb{F}_q$, $a^{-1}(1 - by^2)$ prend $\frac{q+1}{2}$ valeurs

Or : $\frac{q+1}{2} + \frac{q+1}{2} = q + 1 > q = |\mathbb{F}_q|$.
Alors,
il existe $y \in \mathbb{F}_q$ tel que $a^{-1}(1 - by^2) \in \mathbb{F}_q^2$
d'où : $1 = ax^2 + by^2$ avec $x \in \mathbb{F}_q$.

Théorème Soit $\mathbb{F}_q$ un corps de caractéristique différente de 2, et E un $\mathbb{F}_q$ - espace vectoriel de dimension n. Soit $\alpha \in \mathbb{F}_q^*$ tel que $\alpha \notin \mathbb{F}_q^{*2}$. Il y a deux classes d'équivalence de formes quadratiques non dégénérées de E, $Q_1 = \begin{pmatrix} 1 & & (0) \\ & \ddots & \\ (0) & & 1 \end{pmatrix}$ ou $Q_2 = \begin{pmatrix} 1 & & (0) \\ & \ddots 1 & \\ (0) & & \alpha \end{pmatrix}$.

On procède par récurrence sur n.

- si $n = 2$,

on choisit une base orthogonale pour q dans laquelle $q(x, y) = ax^2 + by^2$.
D'après le lemme, il existe un vecteur $e_1 = (x_1, y_1)$ tel que $q(e_1) = 1$
On considère e_2 un vecteur orthogonal à e_1, on a alors :
- si $q(e_2) = \lambda^2 \in \mathbb{F}_q^{*2}$, on pose $e_2' = \lambda^{-1} e_2$ et $q(e_2') = 1$
- sinon, comme $\mathbb{F}_q^{*2}$ est sous-groupe d'indice 2 de $\mathbb{F}_q^*$, il existe $\alpha, \mu \in \mathbb{F}_q^*$ tels que l'on ait $q(e_2) = \alpha \mu^2$. On pose $e_2' = \mu^{-1} e_2$ alors $q(e_2') = \alpha$

- supposons que ce soit vrai au rang $n-1$

On considère $e_1, \dots, e_n$ une base orthogonale.
D'après le lemme, dans $\langle e_1, e_2 \rangle$ il existe ε_1 tel que $q(\varepsilon_1) = 1$
Posons $H = \langle \varepsilon_1 \rangle^\perp$,
alors par hypothèse de récurrence, il existe une base orthogonale $(\varepsilon_2, \dots, \varepsilon_2)$ de $q|_H$ telle que :
$$\operatorname{Mat}_{\tilde{\mathcal{B}}}(q|_H) = \begin{pmatrix} 1 & (0) \\ (0) & 1 \end{pmatrix} \quad \text{ou} \quad \operatorname{Mat}_{\tilde{\mathcal{B}}}(q|_H) = \begin{pmatrix} 1 & & (0) \\ & 1 & \\ (0) & & \alpha \end{pmatrix}$$
Donc,
pour $\mathcal{B} = (\varepsilon_1, \dots, \varepsilon_n)$, $\operatorname{Mat}_{\mathcal{B}}(q) = \begin{pmatrix} 1 & (0) \\ (0) & 1 \end{pmatrix}$ ou $\operatorname{Mat}_{\mathcal{B}}(q) = \begin{pmatrix} 1 & & (0) \\ & 1 & \\ (0) & & \alpha \end{pmatrix}$

Si Q_1 et Q_2 sont semblables,
$\det Q_2 = (\det P)^2 \det Q_1$ i.e. $\alpha = (\det P)^2 \in \mathbb{F}_q^{*2}$: absurde !
Il y a donc deux classes de similitude.