UNIVERSITÉ DE NANTES

FORMATION .....
ANNÉE DE FORMATION .....
ÉPREUVE .....
NOMBRE D'INTERCALAIRES .....

NOM .....
NOM D'USAGE .....
PRÉNOM .....
DATE DE NAISSANCE .....
GROUPE .....
ENSEIGNANT .....
N° ÉTUDIANT .....

Je déclare connaître les suites que pourraient avoir pour moi toute fraude ou tentative de fraude
SIGNATURE

Formes quadratiques sur des corps

NOTE

I) Partie anisotrope

Ne rien inscrire Dans cette marge

F corps (donc principale, local)
X F-espace vectoriel de dim fin
(donc projectif, libre, finiment engendré)
B forme bilinéaire symétrique non-dégénéré
(donc auto-duale)

Seul hypothèse manquante, car $F \neq 2$
↳ rappel: si car $F \neq 2$, X a une base orthogonale

Def: X est anisotrope si
$\forall x \in X \quad x \cdot x = 0 \Rightarrow x = 0$

Lemme: $\exists S$ métabolique, A anisotrope $X = S \oplus A$
Preuve: Par récurrence sur $\dim X$:
Si X anisotrope $X = 0 \oplus X$
Sinon soit $x \in X \quad x \neq 0$ et $x \cdot x = 0$
Comme X est auto-duale, on a $y \in X \quad x \cdot y = 1$
$S_1 = \mathrm{Vect}(x, y) \cong \left\langle \begin{pmatrix} 0 & 1 \\ 1 & * \end{pmatrix} \right\rangle$ est métabolique
$(\mathrm{Vect}(x) = \mathrm{Vect}(x)^{\perp} \subset S_1)$

Ne rien inscrire
Dans cette marge

Comme $S_1 \cap S_1^\perp = \{0\}$, $X \cong S_1 \oplus S_1^\perp$ et on applique l'hypothèse de récurrence à $S_1^\perp$. □

Lemme : Si car $F \neq 2$, cette décomposition est unique à isomorphisme près.

Preuve :

rappel : comme car $F \neq 2$,
S métabolique $\Leftrightarrow S \cong \left\langle \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix} \right\rangle$
$\cong \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle^{\oplus n}$

Donc si $S \oplus A = X = S' \oplus A'$ avec S, S' métaboliques, A, A' anisotrope
$S \cong \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle^{\oplus n}$, $S' \cong \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle^{\oplus n'}$ avec $n \geq n'$

Par théorème de Witt,

$$\underbrace{\left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle^{\oplus (n-n')} \oplus A}_{\text{anisotrope ssi } n = n'} \cong \underbrace{A'}_{\text{anisotrope}}$$

Donc $A \cong A'$ et $S \cong S'$. □

C'est faux si car $F = 2$:

$$\left\langle \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \oplus \langle 1 \rangle$$

$e_1\ e_2\ e_3$; $e_1\ e_2$ métabolique ; e_3 anisotrope

$$= \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \oplus \langle 1 \rangle$$

$e_1+e_3\ \ e_2+e_3$; $e_1+e_2+e_3$

Mais $\left\langle \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \not\cong \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$

↳ totalement isotrope.

Ne rien inscrire
Dans cette marge

Mais en toute caractéristique, la partie anisotrope est bien définie.

$W(F)$ est en bijection avec les classes d'isomorphismes des espaces anisotropes

Cela induit une application

$W(F) \longrightarrow \mathbb{N}$

$w = [A] \longmapsto \|w\| := \dim A$ avec A anisotrope

Propriétés : • $\|w\| = 0 \Rightarrow w = 0$ • $\|1\| = 1$

• $\|w \pm w'\| \leq \|w\| + \|w'\|$ • $\|w w'\| \leq \|w\| . \|w'\|$

II) Corps ordonnés

Ne rien inscrire
Dans cette marge

idée : généralisé le Thm de Sylvester

Def : Un ordre (ordering) / ordonnancement de F est une partie P de F^* tel que
- $\forall x, y \in P \quad x+y \in P$ et $xy \in P$
- $P \cup (-P) = F^*$ ⇝ disjoint car $x + (-x) = 0 \notin P$

P appellé la partie positif de F
P induit un ordre total sur F : $x >_P y$ si $x - y \in P$

- Les carrés sont dans P : x ou $-x \in P$ donc $x^2 = (-x)^2 \in P$
- $n.1 = 1^2 + 1^2 + \dots + 1^2 \in P \subset F^*$ donc $\mathrm{car}(F) = 0$

Thm : (Artin-Schreier)
F est ordonnable si et seulement si
-1 n'est pas une somme de carré (formellement réel)

Preuve : $\Rightarrow$ $-1 = -(1)^2 \notin P$
$x_1^2 + \dots + x_n^2 \in P$

$\Leftarrow$ On considère les ordres partiels $P' \subset F^*$ stable par $+$ et $\times$ et contenant les sommes de carrés.
Par le lemme de Zorn, il y a un ordre partiel P maximal pour l'inclusion
Montrons que P est un ordre (total) sur F.
Il faut voir $P \cup (-P) = F^*$.
Soit $a \in F^*$ et considère $Q = \{x + ay \mid x, y \in P \cup \{0\}, (x,y) \neq (0,0)\}$

Existe car $x_1^2 + \dots + x_k^2 \neq 0$

- Si $0 \notin Q$ et $\exists x, y \in P \quad x + ay = 0$
$-a = \frac{x}{y} = x \cdot y \cdot (y^{-1})^2 \in P$
$\Uparrow P \quad \Uparrow P \quad \Uparrow P$

Ne rien inscrire
Dans cette marge

. Si $a \notin Q$, Q est un ordre partiel contenant P
Par maximalité $Q = P \ni a$ □

$\forall x \in \mathbb{R}\ \exists y \in \mathbb{R}$ $x = y^2$ ou $x = -y^2$

Ex: · $\mathbb{R}$ est ordonné et cet ordre est unique
· $\mathbb{Q}$ est ordonné et cet ordre est unique car

$$0 < \frac{p}{q} = \frac{pq}{q^2} = \sum_{k=1}^{pq} \left(\frac{1}{q}\right)^2 \text{ somme de carrés}$$

· les extensions de $\mathbb{Q}$ contenu dans $\mathbb{R}$
...

Def : X est défini positif si $\forall x \in X \setminus \{0\}.\ x \cdot x \in P$
négatif $\in -P$

Théorème d'inertie (Jacobi, Sylvester) : (X autodual)

$X = X^+ \oplus X^-$ avec X^+ défini positif, X^- défini négatif

De plus $\dim X^+$ et $\dim X^-$ sont un invariant de X.

Preuve : $(e_1, \dots, e_n)$ base orthogonal de X
$X^+ = \mathrm{Vect}(e_i \mid e_i \cdot e_i > 0)$ défini positif
$X^- = \mathrm{Vect}(e_i \mid e_i \cdot e_i < 0)$ défini négatif et $X = X^+ \oplus X^-$

Si $Y \subset X$ défini positif, $Y \cap X^- = \{0\}$ donc
$\dim Y \leq \dim X - \dim X^- = \dim X^+$
Donc $\dim X^+$ est caractérisé comme la dimension maximale d'un sous-espace défini positif de X. □

Def : Signature de X : $\sigma_p(X) = \dim X^+ - \dim X^- \in \mathbb{Z}$.

$$\sigma_p(\langle \alpha \rangle) = \begin{cases} 1 \text{ si } \alpha \in P \\ -1 \text{ si } \alpha \in (-P) \end{cases}$$

UNIVERSITÉ DE NANTES
FORMATION : .....
ANNÉE DE FORMATION : .....
ÉPREUVE : .....

Page n° : .....

NUMÉRO D'ANONYMAT : .....

Ne rien inscrire
Dans cette marge

Lemme : $\sigma_p : W(F) \longrightarrow \mathbb{Z}$ est un morphisme d'anneaux surjectif (= non trivial)

- bien défini : $\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rangle \cong \langle \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} \rangle$ de signature 0 (e_1, e_2 car $\neq 2$; e_1+e_2, e_1-e_2)

donc si S métabolique, $\sigma_p(S) = 0$

Ker σ_p est un idéal premier de $W(F)$

- additivité : $\sigma_p(X \oplus Y) = \sigma_p(X) \oplus \sigma_p(Y)$

- multiplicativité : $X \cong \langle \alpha_1 \rangle \oplus \dots \oplus \langle \alpha_n \rangle$

$\sigma_p(X) = \sigma_p(\langle \alpha_1 \rangle) + \dots + \sigma_p(\langle \alpha_n \rangle)$

d'où

$$\sigma_p(X \otimes Y) = \sigma_p(X) . \sigma_p(Y) \quad \square$$

exc : • $\sigma_p : W(\mathbb{R}) \longrightarrow \mathbb{Z}$ est un iso.

• vrai aussi si F est un corps réel clos

Pour avoir un invariant plus précis, on va considérer l'ensemble des ordres sur F

$\Omega(F) \subset \mathcal{P}(F^*) \simeq \{\pm 1\}^{F^*}$

que l'on munit de la topologie produit

Lemme : $\Omega(F)$ est totalement discontinu, reporté et compact.

Preuve : C'est vrai pour $\{\pm 1\}$

Donc c'est vrai pour le produit $T = \{\pm 1\}^{F^*}$

Il reste à voir que $\Omega(F)$ est un fermé de T.

Ne rien inscrire
Dans cette marge

Soit $f \in T$ qui n'est pas en ordre
alors on a $a, b \in F^*$ tel que
$f(a) = 1 = f(b)$ mais $f(c) = -1$ avec $c = a+b$ ou ab

mais alors
$$\{g \in T \mid g(a) = 1\} \cap \{g \in T \mid g(b) = 1\} \cap \{g \in T \mid g(c) = -1\}$$
est un voisinage ouvert de f ne rencontrant pas $\Omega(F)$
Donc $\Omega(F)$ est fermé. □

Lemme : $\Omega(F) \longrightarrow \mathbb{Z}$ est continue pour tout X.
$P \longmapsto \sigma_P(X)$

$\sigma(X)$ est appellé la signature totale de X

$\sigma(X) \in C^0(\Omega(F), \mathbb{Z})$

$\sigma(X)$ ne dépend que de la classe de Witt de X

On a donc un morphisme d'anneau
$$W(F) \longrightarrow C^0(\Omega(F), \mathbb{Z})$$
$$\sigma : [X] \longmapsto \sigma(X)$$

Application : Si F est une extension algébrique de $\mathbb{Q}$,
$$C^0(\Omega(F), 2\mathbb{Z}) \subseteq Im(\sigma)$$

III) Idéaux premiers de $W(F)$

Si S est métabolique, il est de rang pair

Donc $W(F) \longrightarrow \mathbb{F}_2$ est bien défini
$[X] \longmapsto \dim X \bmod 2$

et son noyau $I(F)$ est un idéal premier appelé l'idéal fondamental de $W(F)$.

Lemme : Si $p \subset W(F)$ premier et $\alpha \in F^*$

alors $\langle \alpha \rangle \equiv \pm \langle 1 \rangle \bmod p$

Preuve : On a $-\langle 1 \rangle = \langle -1 \rangle$ dans $W(F)$

$$(\langle \alpha \rangle + \langle 1 \rangle)(\langle \alpha \rangle - \langle 1 \rangle) = \langle \alpha^2 \rangle - \langle 1^2 \rangle$$
$$= 0 \text{ dans } W(F)$$
$$\left(\langle (\alpha^2) \rangle \overset{e}{\cong} \langle (1) \rangle \right)$$

$W(F)/p$ étant intègre, $\langle \alpha \rangle = \pm \langle 1 \rangle \bmod p$ □

Corollaire : $W(F)/p \cong \mathbb{Z}$ ou $\mathbb{F}_p$

Preuve : $X = \langle \alpha_1 \rangle + \ldots + \langle \alpha_k \rangle$ dans $W(F)$
$X = n \langle 1 \rangle$ dans $W(F)/p$

Donc $\mathbb{Z} \longrightarrow W(F)/p$ surjectif et

$W(F)/p$ est un quotient intègre de $\mathbb{Z}$. □

IV) Noyau et Conoyau de la signature totale

Ne rien inscrire
Dans cette marge

Remarque/Rappel :

$$\begin{array}{ccc} \Omega \times \mathrm{Spec}(\mathbb{Z}) & \longrightarrow & \mathrm{Spec}(W(F)) \\ (P, (q)) & \longmapsto & \ker\left(W(F) \xrightarrow{\sigma_P} \mathbb{Z} \longrightarrow \mathbb{Z}/(q)\right) \end{array}$$

est continue surjective
et injective sauf en $\Omega \times \{(2)\} \longrightarrow I(F)$

Thm : Si -1 n'est pas une somme de carré,
$\ker(\sigma)$ est l'ensemble des nilpotents de $W(F)$
De plus $w \in W(F)$ est inversible si et seulement si
$\sigma(w) \in \mathbb{Z}^{\Omega}$ l'est

Preuve :
- Si $w \in W(F)$ est nilpotent, $\sigma(w) \in \mathbb{Z}^{\Omega}$ est nilpotent
donc $\sigma(w) = 0$
- Si $w \in \ker(\sigma)$ alors $w \in \ker(\sigma_P)$ pour tout
$P \in \Omega(F)$, de plus w est nécessairement de rang
pair donc $w \in I(F)$
Ainsi w est dans tout les idéaux premiers de $W(F)$
donc w est nilpotent
- Si $w \in W(F)$ est inversible, son image $\sigma(w)$ l'est
- Si $\sigma(w)$ est inversible,
$\sigma_P(w) = \pm 1$ et $\sigma_P(w^2) = 1$ pour tout $P \in \Omega$
alors $w^2 - \langle 1 \rangle$ est dans $\ker\sigma$ donc est nilpotent

$$(w^2 - \langle 1 \rangle)^n = 0 \Rightarrow w \cdot \sum_{k=1}^{n} \binom{n}{k} (-1)^{n-k} w^{2k-1} = -\langle 1 \rangle$$

□

Ne rien inscrire
Dans cette marge

Def: On dit que F est euclidien si $(F^*)^2$ est un ordre.

Comparer à $W(F) \simeq \mathbb{F}_2 \iff$ quadratiquement clos $\iff F = F^2$

Prop: $W(F) \simeq \mathbb{Z}$ si et seulement si F est euclidien

Preuve:

- Si F est euclidien, $\langle 1 \rangle$ engendre $W(F)$ donc $W(F) \simeq \mathbb{Z}$
- Si $W(F) \simeq \mathbb{Z}$, F a un ordre P et $\sigma_P : W(F) \xrightarrow{\sim} \mathbb{Z}$ issu

Pour $\alpha \in F^*$

$\sigma_P(\langle \alpha \rangle) = \pm 1 = \sigma_P(\langle \pm 1 \rangle)$ donc $\langle \alpha \rangle = \langle \pm 1 \rangle$

donc α ou $-\alpha$ est un carré. □

Thm (Principe local-global de Pfister):
$\mathrm{Ker}(\sigma)$ est le ss-groupe de torsion de $W(F)$ et ses éléments ont pour ordre une puissance de 2

Preuve:

- $\mathbb{Z}^\Omega$ est sans torsion donc si $w \in W(F)$ est de torsion $\sigma(w) \in \mathbb{Z}^\Omega$ est nul
- Réciproquement soit $w \in W(F)$ tq $\forall n \in \mathbb{N}^*$ $2^n w \neq 0$

On va montrer qu'il a une signature non-triviale.

Une extension de corps $K \setminus F$ induit un morphisme d'anneaux

$$i_K : W(F) \longrightarrow W(K)$$
$$[X] \longmapsto [X \otimes_F K]$$

Considérons $\left\{ K \setminus F \mid \forall n \in \mathbb{N}^* \; 2^n i_K(w) \neq 0 \right\}$

Par le lemme de Zorn, on a une extension maximale K où $2^n i_K(w) \neq 0$.

K est euclidien : Par l'absurde soit $\alpha \in K$ tq α et $-\alpha \notin K^2$.

Par maximalité, on a $n \in \mathbb{N}$ assez grand

$2^n i_{K(\sqrt{\alpha})}(w) = 0$ et $2^n i_{K(\sqrt{-\alpha})}(w) = 0$

Lemme: Si $i_{F(\sqrt{\alpha})}(w) = 0$ alors $w = -\langle \alpha \rangle w$ dans $W(F)$

Ne rien inscrire
Dans cette marge

Donc $2^n i_K(W) = -\langle\alpha\rangle(2^n i_K(W))$
et $2^n i_K(W) = -\langle -\alpha\rangle 2^n i_K(W)$
donc
$2^{n+1} i_K(W) = -(\langle\alpha\rangle + \langle -\alpha\rangle) 2^n i_K(W) = 0$
Contradiction.
Donc K est bien euclidien et a un (unique) ordre P avec $\sigma_P(i_K(W)) \neq 0$
$P \cap F$ défini un ordre sur F tel que $\sigma_{P\cap F}(W) \neq 0$. □

Preuve du lemme :
$W \in W(F)$ tq $i_{F(\sqrt{\alpha})}(W) = 0$ $F(\sqrt{\alpha}) = \{x + \sqrt{\alpha}y ; x, y \in F\}$
Soit X représentant anisotrope de W
$[X \otimes F(\sqrt{\alpha})] = i_{F(\sqrt{\alpha})}(W) = 0$ donc
$\exists\, z = x + \sqrt{\alpha}y \in F(\sqrt{\alpha})$ non nul tel que $z \cdot z = 0$

$x \cdot x + \alpha\, y \cdot y + 2\sqrt{\alpha}\, x \cdot y = 0$
$\begin{cases} x \cdot x + \alpha\, y \cdot y = 0 \\ x \cdot y = 0 \end{cases}$
X étant anisotrope $y \cdot y = \mu \neq 0$ et $x \cdot x = -\alpha\mu \neq 0$
x et y orthogonaux de
$X = \left\langle \begin{pmatrix} \mu & 0 \\ 0 & -\alpha\mu \end{pmatrix} \right\rangle \oplus \mathrm{Vect}(x, y)^{\perp}$
$\qquad\qquad\quad x \qquad\quad y$
$= \langle\mu\rangle \otimes \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -\alpha \end{pmatrix} \right\rangle \oplus \mathrm{Vect}(x, y)^{\perp}$
Par récurrence sur l'orthogonal
$X \cong \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -\alpha \end{pmatrix} \right\rangle \otimes (\langle\mu_1\rangle \oplus \cdots \oplus \langle\mu_k\rangle)$

$\langle -\alpha\rangle \otimes X \cong \left\langle \begin{pmatrix} -\alpha & 0 \\ 0 & \alpha^2 \end{pmatrix} \right\rangle \otimes (\langle\mu_1\rangle \oplus \cdots \oplus \langle\mu_k\rangle)$
$\cong X$ □

Ne rien inscrire
Dans cette marge

Thm : Le conoyau de $\sigma : W(F) \longrightarrow C^0(\Omega(F), \mathbb{Z})$ n'a que des élent d'ordre fini une puissance de 2.

Lemme : Soit $C \subset \Omega(F)$ ouvert et fermé
$\exists n \geq 0$ et $w \in I(F)^n$ tel que $2^n \chi_C = \sigma(w)$
↳ fonction caractéristique

Preuve du lemme :

① Si c'est vrai pour C_1 et C_2 c'est vrai pour $C = C_1 \cup C_2$
On a $2^{m_i} \chi_{C_i} = \sigma(w_i)$ avec $w_i \in I(F)^{m_i}$ $i = 1$ et 2

posons $w_1' = 2^{m_2} w_1$ et $w_2' = 2^{m_1} w_1$ de sorte que
$2^m \chi_{C_i} = \sigma(w_i')$ avec $m = m_1 + m_2$ et $w_i' \in I(F)^m$

$$2^{2m}\chi_C = 2^{2m}\chi_{C_1} + 2^{2m}\chi_{C_2} - 2^{2m}\chi_{C_1}\chi_{C_2}$$
$$= 2^m(\sigma(w_1' + w_2')) - \sigma(w_1' w_2')$$

$$= \sigma(w) \text{ avec } w = 2^m w_1' + 2^m w_2' - w_1' w_2' \in I(F)^{2m}$$

② $C = V_{\alpha_1} \cap \dots \cap V_{\alpha_n}$ avec $V_\alpha = \{P \in \Omega(F) \mid \alpha \in P\}$
$(= \{P \in \Omega(F) \mid -\alpha \notin P\} = U_{-\alpha})$

$$\sigma(\langle 1\rangle + \langle \alpha\rangle) = 2\chi_{V_\alpha}$$
donc pour $w = (\langle 1\rangle + \langle \alpha_1\rangle) \dots (\langle 1\rangle + \langle \alpha_n\rangle)$
$\sigma(w) = 2^n \chi_{V_{\alpha_1}} \dots \chi_{V_{\alpha_n}} = 2^n \chi_C$

③ Les ouverts de $\Omega(F)$ sont les union d'ouvert de la forme $V_{\alpha_1} \cap \dots \cap V_{\alpha_n}$. $\Omega(F)$ étant compact, on peut prendre cette union finie. □

Def : Une forme de Pfister est une forme du type
$(\langle 1\rangle \otimes \langle \alpha_1\rangle) \otimes \dots \otimes (\langle 1\rangle \otimes \langle \alpha_n\rangle)$, $\alpha_i \in F^*$

Ne rien inscrire
Dans cette marge

Preuve du thm du conoyau :

Soit $f \in C^0(\Omega(F), \mathbb{Z})$

$C_i = f^{-1}(\{i\})$ est ouvert et fermé et $\Omega(F) = \coprod_{i \in \mathbb{Z}} C_i$

Par compacité de $\Omega(F)$, il y a un nombre fini de C_i non-vide et donc on peut écrire

$$f = \sum i \chi_{C_i}.$$

Par le lemme on a $2^{n_i} \chi_{C_i} \in \mathrm{Im}(\sigma)$.

Donc pour n assez grand, $2^n f \in \mathrm{Im}(\sigma)$. □

Corollaire : En tant que groupe additif,

$W(F) = \mathrm{Ker}\,\sigma \oplus G$ avec G abélien libre de rg $\mathrm{rg}\, C^0(\Omega, \mathbb{Z})$

↳ torsion puissance de 2

UNIVERSITÉ DE NANTES
FORMATION :
ANNÉE DE FORMATION :
ÉPREUVE :

Page n° :

NUMÉRO D'ANONYMAT :

5) Formes multiplicatives

Ne rien inscrire
Dans cette marge

$\alpha \in F$ est dit représenté (par X) si
$\exists x \in X \quad x \cdot x = \alpha$

Def: X est dit "multiplicatif" si
$X \cong \langle \alpha \rangle \otimes X$ (noté αX)
pour chaque $\alpha \in F^*$ représenté.

Lemme: Si X est multiplicatif, l'ensemble des $\alpha \in F^*$ représenté par X forme un groupe.

Preuve:
- non vide
- Si $\alpha = x \cdot x \neq 0$ et $\beta = y \cdot y \neq 0$.
On a par multiplicativité
$f : X \xrightarrow{\sim} \beta X \quad (= \langle \beta \rangle \otimes X)$

$f(x) = e \otimes z$ avec $e \in \langle \beta \rangle$ et $z \in X$

$\alpha = x \cdot x = f(x) \cdot f(x) = (e \otimes z) \cdot (e \otimes z) = (e \cdot e)(z \cdot z)$
$= \beta z \cdot z$

Donc $\alpha \beta^{-1} = \frac{z}{\lambda} \cdot \frac{z}{\lambda}$ est représenté. □

Ex: $(F^*)^2$ est le groupe associé à la forme multiplicative $\langle 1 \rangle$.

Ex: $\langle 1 \rangle \oplus \langle \alpha \rangle$ est multiplicatif :
Si β est représenté, $\exists y \in F$
$\langle 1 \rangle \oplus \langle \alpha \rangle \cong \langle \beta \rangle \oplus \langle y \rangle$
En prenant le déterminant $\alpha \equiv \beta y \bmod (F^*)^2$
d'où $\alpha\beta \equiv \beta^2 y \equiv y \bmod (F^*)^2$

Ne rien inscrire
Dans cette marge

Donc $\langle\beta\rangle\otimes(\langle 1\rangle\oplus\langle\alpha\rangle) = \langle\beta\rangle\oplus\langle\alpha\beta\rangle = \langle\beta\rangle\oplus\langle\gamma\rangle$
$\cong \langle 1\rangle\oplus\langle\alpha\rangle$.

Thm (Pfister): Si X est multiplicatif et $\alpha\in F$, $(\langle 1\rangle\oplus\langle\alpha\rangle)\otimes X$ est multiplicatif.

Preuve: Soit $\beta\neq 0$ représenté par $(\langle 1\rangle\oplus\langle\alpha\rangle)\otimes X = X\oplus\alpha X$
On a $x,y\in X$ $\beta = \underbrace{x\cdot x}_{\xi} + \alpha\underbrace{y\cdot y}_{\eta}$

ξ et η représentés par X.

- Si $\xi = 0$, $\eta\neq 0$ donc $\eta X = X$

$\beta(X\oplus\alpha X) = (\alpha\eta)(X\oplus\alpha X) = \alpha\eta X\oplus\alpha^2\eta X$
$= \alpha X\oplus X$

- Si $\eta = 0$, $\beta = \xi\neq 0$ donc $\xi X = X$

$\beta(X\oplus\alpha X) = \xi(X\oplus\alpha X) = X\oplus\alpha X$

- Si $\xi,\eta\neq 0$, $\eta X = X$, $\xi X = Y$ et $\frac{\eta}{\xi}X = Y$

$\beta(X\oplus\alpha X) = (\xi+\alpha\eta)(X\oplus\alpha X) = (\xi+\alpha\eta)(X+\alpha\frac{\eta}{\xi}X)$

$= \xi(1+\frac{\alpha\eta}{\xi})(\langle 1\rangle\oplus\langle\alpha\frac{\eta}{\xi}\rangle)\otimes X$

$= \xi(\langle 1\rangle\oplus\langle\frac{\alpha\eta}{\xi}\rangle)\otimes X$ car $1+\frac{\alpha\eta}{\xi}$ représenté par $\langle 1\rangle\oplus\langle\alpha\frac{\eta}{\xi}\rangle$ multiplicatif

$= \xi X + \alpha\eta X$
$= X + \alpha X$ □

Corollaire: Les formes de Pfister sont multiplicatives.

Donc $2^n\langle 1\rangle = (\langle 1\rangle\oplus\langle 1\rangle)\otimes\dots\otimes(\langle 1\rangle\oplus\langle 1\rangle)$
est multiplicatif

UNIVERSITÉ DE NANTES
FORMATION : .....
ANNÉE DE FORMATION : .....
ÉPREUVE : .....

Page n° : .....

NUMÉRO D'ANONYMAT : .....

Ne rien inscrire
Dans cette marge

Corollaire : Dans un corps, un produit de sommes de 2^n carrés est une somme de 2^n carrés.

Mais $15 = 3 \times 5 = (1^2+1^2+1^2)(2^2+1^2+0^2)$
n'est pas somme de 3 carrés dans $\mathbb{Q}$.

Prop : Une forme de 3 fistes est anisotrope ou métabolique

Preuve : Par récurrence sur le rang

- $\langle 1 \rangle \oplus \langle \alpha \rangle$ est anisotrope ou métabolique comme toute forme de rg 2.
- Soit X 3 fistes et $(\langle 1 \rangle \oplus \langle \alpha \rangle) X$ pas anisotrope
Montrer $X + \alpha X = 0$ dans $W(F)$.

$\exists (x,y) \neq 0 \quad \underbrace{x \cdot x}_{\xi} + \alpha \underbrace{y \cdot y}_{\eta} = 0$

- Si ξ ou $\eta = 0$, $x \cdot x$ et $y \cdot y = 0$ et X n'est pas anisotrope donc X, αX et $X \oplus \alpha X$ est métabolique.

- Sinon $-\alpha = \xi/\eta$ est représenté par X multiplicatif

donc $X + \alpha X = (\langle -\alpha \rangle + \langle \alpha \rangle) \otimes X$ est métabolique. □

Def : Le niveau (Stufe) de F est le plus petit entier s tel que -1 est une somme de s carrés
(éventuellement $s = +\infty$)

Ne rien inscrire
Dans cette marge

On montre de manière plus constructif que la coniveau est 2^n ou ∞.

Thm : L'ordre additif de $\langle 1 \rangle$ dans $W(F)$ est 2^s.
De plus $s = 2^n$ ou ∞

Preuve :
$n\langle 1 \rangle$ anisotrope
$\Leftrightarrow x_1^2 + \dots + x_n^2 = 0$ n'a pas de solution non triv
$\Leftrightarrow y_1^2 + \dots + y_{n-1}^2 = -1$ n'a pas de solution
$\Leftrightarrow s > n-1 \Leftrightarrow s \geq n$

- le théorème est donc vrai si $s = +\infty$
- Si s est fini, soit $n \in \mathbb{N}$ tq $2^n \leq s < 2^{n+1}$.
$2^n\langle 1 \rangle$ est anisotrope mais pas $2^{n+1}\langle 1 \rangle$
Donc la forme de Pfister $2^{n+1}\langle 1 \rangle$ est métabolique
Ainsi dans $W(F)$, $2^n\langle 1 \rangle \neq 0$ et $2^{n+1}\langle 1 \rangle = 0$
Donc $\langle 1 \rangle$ est d'ordre 2^{n+1}
Il reste à montrer $s = 2^n$:
$2^{n+1}\langle 1 \rangle = 0 \Leftrightarrow 2^n\langle 1 \rangle = 2^n\langle -1 \rangle$ dans $W(F)$
Puisque les deux sont anisotropes,
$2^n\langle 1 \rangle \cong 2^n\langle -1 \rangle \rightsquigarrow$ représente -1
$2^n\langle 1 \rangle$ représente -1 donc -1 est une somme de 2^n carrés
$s \leq 2^n$. □

UNIVERSITÉ DE NANTES
FORMATION : .....
ANNÉE DE FORMATION : .....
ÉPREUVE : .....

Page n° : .....

NUMÉRO D'ANONYMAT : .....

Ne rien inscrire
Dans cette marge

6) Puissances de l'idéal fondamental

$I = I(F) \subset W(F)$ idéal fondamental forme des forme de rang pair.

I^k est engendré comme groupe additif par les k-formes de Pfister
$(\langle 1\rangle + \langle a_1\rangle)(\langle 1\rangle + \langle a_2\rangle)\dots(\langle 1\rangle + \langle a_k\rangle)$

lien avec la K-théorie

Objectif : étudier la filtration
$\dots \subset I^k \subset \dots \subset I^3 \subset I^2 \subset I \subset W(F)$

- $W(F)/I = \mathbb{F}_2$

  Remarque : Si $w \in I^k$, $2w = (\langle 1\rangle + \langle 1\rangle)w \in I^{k+1}$

- I/I^2

  Si S est métabolique, $S = \left\langle \begin{pmatrix} 0 & I_n \\ I_n & A \end{pmatrix} \right\rangle$
  où $\det S = (-1)^n$
  $\det$ mal défini sur $W(F)$

déterminant signé

Def : Le discriminant de X de rang r est
$d(X) = (-1)^{\frac{r(r-1)}{2}} \det(X)$ mod $(\mathbb{F}^{*})^2$

Si X de rg r, Y de rg s, $d(X \oplus Y) = (-1)^{rs} d(X) d(Y)$

Lemme : d ne dépend que de la classe de Witt
Preuve : si S métabolique, $d(S) = (-1)^n (-1)^n$
et comme S est de rang pair $d(X \oplus S) = (-1)^{rs} d(X) d(S)$
$= d(X)$.

Ne rien inscrire
Dans cette marge

(Pfister)

Thm : $d : (I, +) \to ((F^*)/(F^*)^2, \times)$ est un morphisme de groupe avec $\ker d = I^2$ et surjectif

Preuve : • si $w, w' \in I$ il est de rang pair et $d(w+w') = d(w)\,d(w')$ (morphisme)

• surjectif : $\forall \alpha \in F^*$

$$d(\langle\alpha\rangle + \langle -1\rangle) = (-1)^{\frac{2\times 1}{2}}(-\alpha) = \alpha$$

• $w = (\langle 1\rangle + \langle\alpha\rangle)(\langle 1\rangle + \langle\beta\rangle) = \langle 1\rangle + \langle\alpha\rangle + \langle\beta\rangle + \langle\alpha\beta\rangle$

$$d(w) = \underbrace{(-1)^{\frac{4\times 3}{2}}}_{1}\alpha^2\beta^2 = 1 \bmod (F^*)^2$$

donc $I^2 \subset \ker d$

• Soit $w = \langle\alpha_1\rangle + \ldots + \langle\alpha_{2r}\rangle \in I$ tq $d(w) = 1$

$\langle\alpha\rangle + \langle\beta\rangle = \langle -1\rangle + \langle -\alpha\beta\rangle \bmod I^2$ $\quad w \in I \Rightarrow 2w \in I^2$

$= \langle 1\rangle + \langle\alpha\beta\rangle \bmod I^2$

$$w = \langle 1\rangle + \langle\alpha_1\alpha_2\rangle + \langle\alpha_3\rangle + \ldots + \langle\alpha_{2r}\rangle \bmod I^2$$

$= \ldots$

$= \underbrace{\langle 1\rangle + \ldots + \langle 1\rangle}_{2r-1} + \langle\xi\rangle \bmod I^2$ $\quad \xi = \alpha_1\alpha_2\ldots\alpha_{2r}$

$= 3\langle 1\rangle + \langle\xi\rangle$ ou $\langle 1\rangle + \langle\xi\rangle \bmod I^2$

$4\langle 1\rangle \in I^2$

$= \langle 1\rangle + \langle\xi\rangle$ quitte à changer ξ en $-\xi$

donc $1 = d(w) = -\xi \bmod (F^*)^2$

$w = \langle 1\rangle + \langle\xi\rangle = \langle -\xi\rangle + \langle\xi\rangle = 0 \bmod (F^*)^2$ □

• I^2/I^3

Def : Un symbole de Steinberg sur F est une application $\varphi : F^* \times F^* \longrightarrow \{\pm 1\}$ multiplicative à gauche et à droite tel que $\varphi(\alpha, \beta) = 1$ si $\alpha + \beta = 1$

UNIVERSITÉ DE NANTES
FORMATION : .....
ANNÉE DE FORMATION : .....
ÉPREUVE : .....

Page n° : .....

NUMÉRO D'ANONYMAT : .....

Ne rien inscrire
Dans cette marge

Pour φ symbole $(\pm 1)^2$

- $\varphi(\gamma^2\alpha, \beta) = \varphi(\gamma, \beta)^2 \varphi(\alpha, \beta) = \varphi(\alpha, \beta)$
- $\varphi(\alpha^{-1}, \beta) = \varphi(\alpha, \beta)$
- $1 = \varphi(\alpha, 1-\alpha) = \varphi(\alpha, -\alpha(1-\alpha^{-1}))$
  $= \varphi(\alpha, -\alpha)\, \varphi(\alpha, 1-\alpha^{-1}) = \varphi(\alpha, -\alpha)\, \varphi(\alpha^{-1}, 1-\alpha^{-1})$
  $= \varphi(\alpha, -\alpha)$
- $\varphi(\alpha, \beta) = \varphi(\beta, \alpha)$: $1 = \varphi(\alpha\beta, -\alpha\beta) = \varphi(\alpha, -\alpha)\, \varphi(\alpha, \beta)\, \varphi(\beta, \alpha)\, \varphi(\beta, -\beta)$
  $= 1$

Lemme : Si $\langle\alpha\rangle + \langle\beta\rangle \simeq \langle\alpha'\rangle + \langle\beta'\rangle$ dans $W(F)$
alors $\varphi(\alpha, \beta) = \varphi(\alpha', \beta')$

Preuve : • Si $\langle\alpha\rangle + \langle\beta\rangle$ est métabolique
$\exists x, y \neq (0,0) \quad \alpha x^2 + \beta y^2 = 0 \rightsquigarrow \alpha = -\beta\left(\frac{y}{x}\right)^2$
$\varphi(\alpha, \beta) = \varphi(-\beta\left(\frac{x}{y}\right)^2, \beta) = \varphi(-\beta, \beta) = 1$

• Si $\langle\alpha\rangle + \langle\beta\rangle = \langle\alpha'\rangle + \langle\beta'\rangle \neq 0$
$\langle\alpha\rangle \oplus \langle\beta\rangle \cong \langle\alpha'\rangle \oplus \langle\beta'\rangle$

On a $(x, y) \neq (0,0) \quad \alpha x^2 + \beta y^2 = \alpha'$
Si $y = 0$, $\alpha = \alpha' \bmod (F^*)^2$
et comme $\alpha\beta = \det = \alpha'\beta' \bmod (F^*)^2$
$\beta = \beta' \bmod (F^*)^2$
Donc $\varphi(\alpha, \beta) = \varphi(\alpha', \beta')$
De même si $x = 0$.
Si $x, y \neq 0$
$\varphi(\alpha\alpha', \beta\alpha') = \varphi(\alpha\frac{x^2}{\alpha'}, \frac{\beta y^2}{\alpha'}) = 1$ car $\frac{\alpha x^2 + \beta y^2}{\alpha'} = 1$

Ne rien inscrire
Dans cette marge

$\varphi(\alpha,\beta)\varphi(\alpha',\beta') = \varphi(\alpha,\beta)\varphi(\alpha',\alpha\beta\alpha')$ car $\alpha\beta \equiv \alpha'\beta' \bmod (F^*)^2$
$= \varphi(\alpha,\beta)\,\varphi(\alpha',\alpha)\,\varphi(\alpha',\beta\alpha')$
$= \varphi(\alpha,\beta)\,\varphi(\alpha,\alpha')\,\varphi(\alpha',\beta\alpha')$
$= \varphi(\alpha,\beta\alpha')\,\varphi(\alpha',\beta\alpha') = \varphi(\alpha\alpha',\beta\alpha') = 1$

□

Invariant de Hasse

Pour $X \cong \langle\alpha_1\rangle \oplus \dots \langle\alpha_n\rangle \oplus N$ symplectique si $\dim = 2$

$H_\varphi(X) = \prod_{i<j} \varphi(\alpha_i,\alpha_j) \in \{\pm 1\}$

Thm : Si X et Y ont même rang et classe de Witt alors $H_\varphi(X) = H_\varphi(Y)$

Si $X = \langle\alpha_1\rangle \oplus \dots \oplus \langle\alpha_n\rangle$ et $Y = \langle\beta_1\rangle \oplus \dots \oplus \langle\beta_n\rangle$ tq
$\exists i_1, i_2$ $\langle\alpha_{i_1}\rangle \oplus \langle\alpha_{i_2}\rangle \cong \langle\beta_{i_1}\rangle \oplus \langle\beta_{i_2}\rangle$ et
$\alpha_i = \beta_i$ pour $i \neq i_1, i_2$ alors on note $X \sim Y$
On complète cette relation par transitivité à toutes les formes diagonales.

Thm d'équivalence en classe de Witt :
$X \cong Y$ si et seulement si $X \sim Y$
Preuve : $\Leftarrow$ clair
$\Rightarrow$ Par récurrence sur le rang de $X \cong Y$
X représente β_1
Soit $X' \sim X$ tel que $X' = \langle\gamma_1\rangle \oplus \dots \oplus \langle\gamma_n\rangle$ avec p minimal tel que
$\exists x_1, \dots, x_p \in F$ $\beta_1 = \gamma_1 x_1^2 + \dots + \gamma_p x_p^2$

On a en fait $p = 1$. (x_1, x_2) $(x_1, x_2)^\perp$
Si $a = \gamma_1 x_1^2 + \gamma_2 x_2^2$: $\langle\gamma_1\rangle \oplus \langle\gamma_2\rangle \cong \langle a\rangle \oplus \langle b\rangle$
Donc $X \sim X' \sim \langle a\rangle \oplus \langle b\rangle \oplus \langle\gamma_3\rangle \oplus \dots \oplus \langle\gamma_n\rangle$
$\sim \langle a\rangle \oplus \langle\gamma_3\rangle \oplus \dots \oplus \langle\gamma_n\rangle \oplus \langle b\rangle$

avec $\beta_1 = a + \gamma_3 x_3^2 + \dots + \gamma_n x_n^2$

Ne rien inscrire
Dans cette marge

Donc $p=1$ et $\langle \gamma_1 \rangle$ repond $\langle \beta_1 \rangle$ si $\langle \gamma_1 \rangle \cong \langle \beta_2 \rangle$

$\langle \beta_1 \rangle \oplus \dots \oplus \langle \beta_n \rangle = Y \cong X \sim \langle \gamma_1 \rangle \oplus \dots \oplus \langle \gamma_n \rangle$

$\Downarrow$ Witt?

$\langle \beta_2 \rangle \oplus \dots \oplus \langle \beta_n \rangle \cong \langle \gamma_2 \rangle \oplus \dots \oplus \langle \gamma_n \rangle$

Et par hypothèse de recurrence $\langle \beta_2 \rangle \oplus \dots \oplus \langle \beta_n \rangle \sim \langle \gamma_2 \rangle \oplus \dots \oplus \langle \gamma_n \rangle$ □

Preuve invariant:

Si $X \cong Y$, on peut supposer

$X = \langle \alpha_1 \rangle \oplus \langle \alpha_2 \rangle \oplus \langle \alpha_3 \rangle \dots \oplus \langle \alpha_n \rangle$ avec $\langle \alpha_1 \rangle \oplus \langle \alpha_2 \rangle \cong \langle \alpha_1' \rangle \oplus \langle \alpha_2' \rangle$

$Y = \langle \alpha_1' \rangle \oplus \langle \alpha_2' \rangle \oplus \langle \alpha_3 \rangle \dots \oplus \langle \alpha_n \rangle$

On a vu $\gamma(\alpha_1, \alpha_2) = \gamma(\alpha_1', \alpha_2')$ et (det)

$\gamma(\alpha_1, \alpha_i)\gamma(\alpha_2, \alpha_i) = \gamma(\alpha_1\alpha_2, \alpha_i) = \gamma(\alpha_1'\alpha_2', \alpha_i) =$

$= \gamma(\alpha_1', \alpha_i)\gamma(\alpha_2', \alpha_i)$ □

$H_\gamma(X \oplus Y) = \prod_{i<j} \gamma(\alpha_i, \alpha_j) \prod_{k<l} \gamma(\beta_k, \beta_l) \prod_{i,k} \gamma(\alpha_i, \beta_k)$

$= H_\gamma(X) H_\gamma(Y) \prod_i \gamma(\alpha_i, \prod_k \beta_k)$

$= H_\gamma(X) H_\gamma(Y) \gamma(\prod_i \alpha_i, \prod_k \beta_k) = H_\gamma(X) H_\gamma(Y) \gamma(\det X, \det Y)$

- Si S métabolique, $S = \overbrace{\langle 1 \rangle + \dots + \langle 1 \rangle}^{n} + \overbrace{\langle -1 \rangle + \dots + \langle -1 \rangle}^{n}$

dim $W(F)$ et $n \geq 2$

$\gamma(1,1) = \gamma(1,-1) = \gamma(-1,1) = 1$ obs

$H_\gamma(S) = \gamma(-1,-1)^{\frac{n(n-1)}{2}} = 1$ si $\frac{n(n-1)}{2}$ pair

si $\operatorname{rg} S = 0 \bmod 4$

UNIVERSITÉ DE NANTES
FORMATION :
ANNÉE DE FORMATION :
ÉPREUVE :

Page n° :

NUMÉRO D'ANONYMAT :

$$I^3 \xrightarrow{?} I^2 \xrightarrow{(F^*/(F^*)^2} I(F) \xrightarrow{F_2} W(F)$$

Ne rien inscrire
Dans cette marge

Rappel :

- $\varphi : F^* \times F^* \longrightarrow \{\pm 1\}$ symbole
si bimultiplicatif et $\alpha + \beta = 1 \Rightarrow \varphi(\alpha, \beta) = 1$

- Etant donné un symbole φ et une forme diagonale
$X = \langle \alpha_1 \rangle \oplus \dots \oplus \langle \alpha_n \rangle$

invariant de Hasse : $H_\varphi(X) = \prod_{i<j} \varphi(\alpha_i, \alpha_j) \in \{\pm 1\}$

On a montrer $X \cong Y \Rightarrow H_\varphi(X) = H_\varphi(Y)$

Objectif : ① passer au dasse de Witt
② faire le lien avec I^2/I^3

①

- $S = \overbrace{\langle 1 \rangle + \dots + \langle 1 \rangle}^{n} + \overbrace{\langle -1 \rangle + \dots + \langle -1 \rangle}^{n}$

$\varphi(1,1) = \varphi(1,-1) = \varphi(-1,1) = 1$ donc

$H_\varphi(S) = \varphi(-1,-1)^{\frac{n(n-1)}{2}}$

$= 1$ SI $\frac{n(n-1)}{2}$ pair

← en particulier si $\operatorname{rg} S \equiv 0 \bmod 8$

dans ce cas $\det(S) = 1$

- Si $X = \langle \alpha_1 \rangle \oplus \dots \oplus \langle \alpha_n \rangle$ et $Y = \langle \beta_1 \rangle \oplus \dots \oplus \langle \beta_m \rangle$

$$H_\varphi(X \oplus Y) = \prod_{i<j} \varphi(\alpha_i, \alpha_j) \prod_{i<j} \varphi(\beta_i, \beta_j) \prod_{i,k} \varphi(\alpha_i, \beta_k)$$

$$= H_\varphi(X) H_\varphi(Y) \varphi\left(\prod_i \alpha_i, \prod_k \beta_k\right)$$

Ne rien inscrire
Dans cette marge

$$h_\varphi(X \oplus Y) = h_\varphi(X) h_\varphi(Y) \varphi(\det X, \det Y)$$

Def: Soit $w \in I(F)$ représenté par X de rang multiple de 8,
l'invariant de Hasse-Witt de w est

$$h_\varphi(w) := H_\varphi(X) \in \{\pm 1\}.$$

Bien défini ok ✓

(II) **Thm:** $h_\varphi : I^2(F) \longrightarrow \{\pm 1\}$ est un morphisme de groupe.

Preuve:

$$h_\varphi(w+w') = H_\varphi(X \oplus X') = H_\varphi(X) H_\varphi(X') \varphi(\det X, \det X')$$
$$= h_\varphi(w) h_\varphi(w') \varphi(d(w), d(w'))$$

$d(X) = (-1)^{\frac{r(r-1)}{2}} \det X$

On a $d(w) = 1 \Leftrightarrow w \in I^2$
donc $h_\varphi(w+w') = h_\varphi(w) h_\varphi(w')$ □

Thm: $\operatorname{Hom}_{\text{Grp}}\left(\frac{I^2}{I^3}, \{\pm 1\}\right) = \{h_\varphi \text{ , } \varphi \text{ symbole}\}$

Preuve: ⊃ On vérifie pour les 3-fermes de Pfister

Lemme: $h_\varphi(\langle\beta\rangle w) = h_\varphi(w) \varphi(d(w), \beta)$ $w \in I$

$w = \langle\alpha_1\rangle + \ldots + \langle\alpha_n\rangle$ $n \equiv 0 \bmod 8$

$$h_\varphi(\langle\beta\rangle w) = \prod_{i<j} \varphi(\beta a_i, \beta a_j) = \prod_{i<j} \left(\varphi(\alpha_i, \alpha_j) \varphi(\beta, \alpha_i) \varphi(\beta, \alpha_j) \varphi(\beta, \beta)\right)$$
$$= h_\varphi(w) \varphi(\beta, \beta)^{\frac{n(n-1)}{2}} \left(\prod_i \varphi(\alpha_i, \beta)\right)^{n-1}$$
$$= h_\varphi(w) \varphi(\prod \alpha_i, \beta) = h_\varphi(w) \varphi(d(w), \beta)$$

□

UNIVERSITÉ DE NANTES
FORMATION :
ANNÉE DE FORMATION :
ÉPREUVE :

Page n° :

NUMÉRO D'ANONYMAT :

Ne rien inscrire
Dans cette marge

Donc pour $w = (\langle 1\rangle + \langle\beta\rangle)\underbrace{(\langle 1\rangle + \langle\alpha_1\rangle)(\langle 1\rangle + \langle\alpha_2\rangle)}_{w' \in I^2}$

$h_\varphi(\langle\beta\rangle w') = h_\varphi(w')\varphi(d(w'), \beta) = h_\varphi(w')$ ($d(w') = 1$)

$h_\varphi(w) = h_\varphi(w' + \langle\beta\rangle w') = h_\varphi(w')\, h_\varphi(w') = 1$ ($(\pm 1)^2$)

C : Soit $g : \frac{I^2}{I^3} \longrightarrow \{\pm 1\}$ morphisme

On pose $\varphi(\alpha, \beta) = g((\langle\alpha\rangle - \langle 1\rangle)(\langle\beta\rangle - \langle 1\rangle))$

$(\langle\alpha\rangle - \langle 1\rangle)(\langle\alpha'\rangle - \langle 1\rangle) = \langle\alpha\alpha'\rangle - \langle\alpha\rangle - \langle\alpha'\rangle + \langle 1\rangle$
$= 0 \bmod I^2$

$\langle\alpha\alpha'\rangle - \langle 1\rangle = \langle\alpha\rangle - \langle 1\rangle + \langle\alpha'\rangle - \langle 1\rangle \bmod I^2$

$(\langle\alpha\alpha'\rangle - \langle 1\rangle)(\langle\beta\rangle - \langle 1\rangle) =$
$(\langle\alpha\rangle - \langle 1\rangle)(\langle\beta\rangle - \langle 1\rangle) + (\langle\alpha'\rangle - \langle 1\rangle)(\langle\beta\rangle - \langle 1\rangle) \bmod I^3$

Donc φ est bimultiplicative

Si $\alpha + \beta = 1$, $\langle\alpha\rangle \oplus \langle\beta\rangle \cong \langle 1\rangle \oplus \langle\alpha\beta\rangle$
donc $(\langle\alpha\rangle - \langle 1\rangle)(\langle\beta\rangle - \langle 1\rangle) = 0$
donc φ est un symbole

On vérifie $g = h_\varphi$ sur les générateurs $(\langle\alpha\rangle - \langle 1\rangle)(\langle\beta\rangle - \langle 1\rangle)$

$h_\varphi(w) = h_\varphi(\langle\alpha\beta\rangle + \langle -\alpha\rangle + \langle -\beta\rangle + \langle 1\rangle)$
$= h_\varphi(\langle\alpha\beta\rangle + \langle -\alpha\rangle + \langle -\beta\rangle + \langle 1\rangle + \langle 1\rangle + \langle 1\rangle + \langle 1\rangle + \langle -1\rangle)$
$= \varphi(\alpha\beta, -\alpha)\varphi(\alpha\beta, -\beta)\varphi(-\alpha, -\beta)\varphi(-1, -1)$
$= \varphi(\alpha, -\alpha)\varphi(\beta, -\alpha)\varphi(-\alpha^2\beta, -\beta)\varphi(-1, -1)$
$= \varphi(\beta, -\alpha)\varphi(-\beta, -\beta)\varphi(-1, -1)$
$= \varphi(\beta, \alpha)\varphi(\beta, -1)\varphi(-\beta, -1)\varphi(-\beta, \beta)\varphi(-1, -1) = \varphi(\alpha, \beta)$ □