

# ANNALES SCIENTIFIQUES DE L'É.N.S.

MICHEL BROUÉ

MICHEL ENGUEHARD

**Une famille infinie de formes quadratiques entières ; leurs groupes d'automorphismes**

*Annales scientifiques de l'É.N.S. 4<sup>e</sup> série*, tome 6, n° 1 (1973), p. 17-51

[http://www.numdam.org/item?id=ASENS\\_1973\\_4\\_6\\_1\\_17\\_0](http://www.numdam.org/item?id=ASENS_1973_4_6_1_17_0)

© Gauthier-Villars (Éditions scientifiques et médicales Elsevier), 1973, tous droits réservés.

L'accès aux archives de la revue « Annales scientifiques de l'É.N.S. » (<http://www.elsevier.com/locate/ansens>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques  
<http://www.numdam.org/>

# UNE FAMILLE INFINIE DE FORMES QUADRATIQUES ENTIÈRES; LEURS GROUPES D'AUTOMORPHISMES

PAR MICHEL BROUÉ ET MICHEL ENGUEHARD

---

## INTRODUCTION

Nous étudions ici une famille remarquable de formes quadratiques entières définies positives  $(\Phi_d)_{d \geq 1}$ . La forme  $\Phi_d$ , en  $2^d$  variables, est définie par un réseau  $U(d)$  dans  $\mathbf{Q}^{2^d}$ , pair, contenu dans son dual, unimodulaire si  $d$  est impair. L'un des intérêts de ces réseaux est qu'ils ont de « gros » groupes d'automorphismes dont la construction, l'étude et la structure ne peuvent que rappeler la construction, l'étude et la structure du groupe de Conway [4]. Les vecteurs non nuls de longueur minimale de  $U(d)$  sont de carré  $2^m$ ,  $m$  étant la partie entière de  $\frac{d}{2}$ . L'opération du groupe  $G(d)$  des automorphismes de  $U(d)$  sur ces vecteurs est transitive et elle montre que, si  $d$  est supérieur ou égal à 4,  $G(d)/\{-1, +1\}$  est extension d'un 2-groupe abélien élémentaire d'ordre  $2^{2d}$  par le groupe simple de Chevalley de type  $D_d$  sur le corps  $\mathbf{F}_2$ . La représentation ainsi obtenue du groupe de Chevalley est isomorphe à sa représentation naturelle comme groupe orthogonal, et l'extension n'est pas scindée.

Ces résultats ont été annoncés dans [3].

Le chapitre I est consacré à quelques propriétés générales des réseaux dans  $\mathbf{Q}^n$  en particulier aux chaînes d'espaces vectoriels qu'ils définissent (§ 1) et à l'étude de certains sous-espaces de  $(\mathbf{F}_2)^{2^d}$ , dits « codes affines » (§ 2). Au chapitre II sont construits et étudiés à partir des codes affines les réseaux  $U(d)$ .

Afin que le texte ne soit pas trop long, certaines démonstrations élémentaires sont laissées au lecteur. Pour le chapitre I, on pourra se rapporter à [2].

## CHAPITRE I

1. SUR LES RÉSEAUX DE  $\mathbf{Q}^n$ .1.1. Quelques définitions. — Soit  $n$  un entier positif.

L'espace vectoriel  $\mathbf{Q}^n$  est supposé muni de sa forme bilinéaire canonique, notée  $(x, y) \mapsto x.y$ , forme pour laquelle la base canonique est orthonormale.

DÉFINITION I.1. — Un réseau de  $\mathbf{Q}^n$  — ou plus simplement réseau — est un sous- $\mathbf{Z}$ -module de  $\mathbf{Q}^n$ , libre de rang  $n$ , muni du produit scalaire induit.

DÉFINITION I.2. — Soit  $L$  un réseau de  $\mathbf{Q}^n$ . Le dual de  $L$ , noté  $L^0$ , est le  $\mathbf{Z}$ -module des éléments  $x$  de  $\mathbf{Q}^n$  tels que  $x.y \in \mathbf{Z}$  quel que soit  $y$  appartenant à  $L$ . Il s'identifie canoniquement à  $\text{Hom}(L, \mathbf{Z})$ .

DÉFINITION I.3. — Le volume d'un réseau  $L$ , noté  $\text{vol}(L)$ , est la valeur absolue du déterminant des vecteurs d'une base de  $L$  par rapport à la base canonique de  $\mathbf{Q}^n$ .

DÉFINITION I.4. — Soit  $r$  un nombre rationnel positif. Un réseau  $L$  est dit  $r$ -modulaire si  $L^0 = rL$ . Un réseau 1-modulaire est dit unimodulaire.

Les propriétés suivantes sont bien connues (cf. [5]) et sont citées pour mémoire :

PROPOSITION I.1. — Soient  $L$  et  $L'$  deux réseaux de  $\mathbf{Q}^n$ . Alors :

(1)  $L^0$  est un réseau,  $(L^0)^0 = L$  et  $\text{vol}(L).\text{vol}(L^0) = 1$ .

(2) Si  $L$  est  $r$ -modulaire,  $\text{vol}(L) = r^{-\frac{n}{2}}$ .

(3)  $L \cap L'$  et  $L + L'$  sont des réseaux et on a

$$(L \cap L')^0 = L^0 + L'^0 \quad \text{et} \quad (L + L')^0 = L^0 \cap L'^0.$$

(4) Si  $L \subset L'$ ,  $L'^0 \subset L^0$  et  $L'/L$  est canoniquement isomorphe à  $L^0/L'^0$ .

(5) Si  $\{e_i\}_{i=1,2,\dots,n}$  est une base de  $L$ , la base duale  $\{e_i^0\}_{i=1,2,\dots,n}$  dans  $\mathbf{Q}^n$  est une base de  $L^0$ .

DÉFINITION I.5. — Soit  $r$  un nombre rationnel positif et soit  $L$  un réseau. Si  $L$  admet une base orthogonale formée de vecteurs de carré  $r^{-1}$ ,  $L$  est  $r$ -modulaire et dit «  $r$ -modulaire trivial ».

D'après la définition I.1, un automorphisme d'un réseau  $L$  de  $\mathbf{Q}^n$  est une transformation orthogonale de  $\mathbf{Q}^n$  qui fixe globalement  $L$ .

**PROPOSITION I.2.** — Soit  $L$  un réseau  $r$ -modulaire trivial de base orthogonale  $\{e_j\}_{1 \leq j \leq n}$ . Le groupe des automorphismes de  $L$  est produit semi-direct d'un groupe abélien élémentaire d'ordre  $2^n$ , le groupe des transformations  $s$  telles que  $s(e_j) = \pm e_j$  pour tout  $j$ , par un groupe isomorphe au groupe symétrique de degré  $n$ , le groupe des transformations qui permutent les  $e_j$  ( $1 \leq j \leq n$ ).

**1.2. Réduction modulo 2 et dualité. Cas des réseaux  $r$ -modulaires.** — Si  $n$  est un entier, sa classe modulo 2 sera notée  $n$ .

Si  $L$  est un réseau de  $\mathbf{Q}^n$ , la surjection canonique de  $L$  sur  $L/2L$  sera notée  $\varphi_L$ . Nous poserons  $\varphi_L(x) = \bar{x}$ , pour  $x \in L$ .

Le groupe abélien  $L/2L$  peut être identifié à  $\mathbf{F}_2 \otimes_{\mathbf{Z}} L$  et considéré comme un espace vectoriel sur  $\mathbf{F}_2$ .

Le dual  $L^0$  de  $L$  s'identifiant canoniquement à  $\text{Hom}(L, \mathbf{Z})$ ,  $L^0/2L^0$  s'identifie à  $\mathbf{F}_2 \otimes \text{Hom}(L, \mathbf{Z})$  donc aussi à  $\text{Hom}(L/2L, \mathbf{F}_2)$ , dual relativement à  $\mathbf{F}_2$  de  $L/2L$ . Le couplage ainsi défini entre  $L/2L$  et  $L^0/2L^0$  est tel que si  $x \in L$  et  $y \in L^0$ ,  $(\bar{x}, \bar{y}) = \overline{x \cdot y}$ .

Si  $V$  est un sous-espace vectoriel de  $L/2L$ , son orthogonal dans  $L^0/2L^0$  [identifié à  $\text{Hom}(L/2L, \mathbf{F}_2)$ ] sera noté  $V^\perp$ .

Supposons maintenant que  $L$  soit un réseau  $r$ -modulaire :  $L^0 = rL$ . La multiplication par  $r$ , que nous noterons  $\mu_r$ , définit donc un isomorphisme canonique de  $L$  sur  $L^0$  (isomorphisme de groupes abéliens). Par réduction modulo 2,  $\mu_r$  définit un isomorphisme d'espaces vectoriels sur  $\mathbf{F}_2$ , soit  $\bar{\mu}_r$ , de  $L/2L$  sur  $L^0/2L^0$ , tel que le diagramme suivant soit commutatif

$$\begin{array}{ccc} L & \xrightarrow{\mu_r} & L^0 \\ \varphi_L \downarrow & & \downarrow \varphi_{L^0} \\ L/2L & \xrightarrow{\bar{\mu}_r} & L^0/2L^0 \end{array}$$

Cet isomorphisme induit, par composition avec l'isomorphisme de  $L^0/2L^0$  sur  $\text{Hom}(L/2L; \mathbf{F}_2)$  établi plus haut, un produit scalaire sur  $L/2L$ , appelé produit scalaire naturel sur  $L/2L$ .

**Convention.** — Si  $V$  est un sous-espace vectoriel (sur  $\mathbf{F}_2$ ) de  $L/2L$ , l'orthogonal de  $V$  pour le produit scalaire naturel dans  $L/2L$  sera noté  $V^0$ .

**PROPOSITION I.3.** — Soit  $L$  un réseau  $r$ -modulaire.

(1) Supposons que  $L$  soit trivial. Soit  $\Omega_L$  l'image commune dans  $L/2L$  des bases orthogonales de  $L$ . Alors  $\Omega_L$  est une base orthogonale de  $L/2L$  pour le produit scalaire naturel.

(2) *Supposons que  $L$  soit unimodulaire. Le produit scalaire naturel sur  $L/2L$  est égal au produit scalaire induit sur  $L/2L$  par réduction modulo 2 de la restriction à  $L$  du produit scalaire de  $\mathbf{Q}^n$ .*

1.3. *Réseaux contenus dans un réseau  $2^m$ -modulaire trivial.* — L'étude des cas particuliers envisagés dans ce paragraphe est justifiée par le théorème suivant, essentiellement dû à Kneser :

**THÉORÈME I.1.** — *Soit  $U$  un réseau de  $\mathbf{Q}^n$  ( $n \geq 5$ ). Si  $U \subset U^0$ , il existe un entier  $m$  et un réseau  $2^m$ -modulaire trivial  $R$  tel que  $U \subset R$  et  $2^m R \subset U^0$ .*

*Démonstration du théorème I.1.* — Si  $U \subset R$ , où  $R$  est  $2^m$ -modulaire trivial, on a [proposition I.1 (4)],  $R^0 \subset U^0$ , soit  $2^m R \subset U^0$ .

Démontrons d'abord le théorème I.1 dans le cas où  $U$  est unimodulaire. Soit  $L_n$  le réseau unimodulaire de  $\mathbf{Q}^n$  engendré par la base canonique de  $\mathbf{Q}^n$ . D'après la proposition 106.2 de [5], il existe une transformation orthogonale  $\sigma$  de  $\mathbf{Q}^n$ , une base  $a_1, \dots, a_n$  de  $L_n$  et des entiers relatifs  $r_1 \leq r_2 \leq \dots \leq r_n$  tels que  $\sigma(U)$  admette pour base l'ensemble des  $2^{r_j} a_j$ . Alors  $\sigma(U) \subset 2^{r_1} L_n$ . En outre  $2^{r_1} L_n$  est un réseau  $2^{-2r_1}$ -modulaire trivial. On a  $U \subset \sigma^{-1}(2^{r_1} L_n)$ .

Supposons maintenant que  $U \subset U^0$ . Soit  $L$  un réseau unimodulaire de  $\mathbf{Q}^n$ . Posons  $V = (L + U) \cap U^0$ . On a, d'après la proposition I.1,

$$V^0 = (L + U)^0 + U^{00} = (L^0 \cap U^0) + U = (L + U) \cap U^0 \quad (\text{car } U \subset U^0);$$

Donc  $V = V^0$  et il existe un entier  $m$  et un réseau  $2^m$ -modulaire trivial  $R$  tel que  $V \subset R$ . Mais  $U \subset V$ , donc  $U \subset R$ .

*Notations et hypothèses.* — Nous supposerons maintenant que  $R$  est un réseau  $2^m$ -modulaire trivial et  $U$  un réseau tel que

$$2^m R \subset U \subset U^0 \subset R.$$

Pour tous entiers  $\alpha$  et  $\beta$ , posons

$$\begin{aligned} \bar{U}_\alpha(R) &= \varphi_R(2^{-\alpha} U \cap R) \subset R/2R, & \bar{U}_\alpha^0(R) &= \varphi_R(2^{-\alpha} U^0 \cap R) \subset R/2R, \\ \bar{R}^\beta(U) &= \varphi_U(2^\beta R \cap U) \subset U/2U, & \bar{R}^\beta(U^0) &= \varphi_{U^0}(2^\beta R \cap U^0) \subset U^0/2U^0. \end{aligned}$$

**THÉORÈME I.2.** — *Sous les hypothèses et avec les notations précédentes :*

(1) *dans  $R/2R$  muni du produit scalaire naturel,*

$$\bar{U}_\alpha(R)^0 = \bar{U}_{m-(\alpha+1)}^0(R);$$

(2)  *$U^0/2U^0$  étant identifié au dual de  $U/2U$ ,*

$$\bar{R}^\beta(U)^\perp = \bar{R}^{m-\beta+1}(U^0);$$

Si  $U$  est unimodulaire, dans  $U/2U$  muni du produit scalaire naturel

$$\overline{R}^\beta(U)^0 = \overline{R}^{m-\beta+1}(U);$$

$$(3) [\overline{U}_\alpha(R) : \mathbf{F}_2] = [\overline{R}^{m-\alpha}(U^0) : \mathbf{F}_2] = n - [\overline{R}^{\alpha+1}(U) : \mathbf{F}_2].$$

**THÉORÈME I.3.** (*Hypothèses du théorème I.2.*) — *Volume de  $U$  :* Soit  $\delta_\alpha$  la dimension de  $\overline{U}_\alpha(R)$  sur  $\mathbf{F}_2$ , pour  $\alpha = 0, 1, \dots, m-1$ . On a  $\text{vol}(U) = 2^{\frac{mn}{2} - \sum \delta_\alpha}$  (somme de 0 à  $m-1$ ).

**COROLLAIRE 1.** — Soient  $V$  et  $V'$  deux réseaux tels que

$$2^m R \subset V \subset V' \subset R.$$

Si  $\overline{V}_\alpha(R) = \overline{V}'_\alpha(R)$  pour tout  $\alpha$  entre 0 et  $m$ ,  $V = V'$ .

**COROLLAIRE 2.** — *Génération.* (Notations et hypothèses du théorème 1.) Soit pour tout entier  $\alpha$  entre 0 et  $m$  une famille  $\mathcal{G}(\alpha)$  de vecteurs de  $R \cap 2^{-\alpha}U$  telle que  $\varphi_R(\mathcal{G}(\alpha))$  engendre  $\overline{U}_\alpha(R)$ , Soit pour tout entier  $k$  entre 0 et  $m$ ,  $L_k$  le sous- $\mathbf{Z}$ -module engendré par  $\bigcup_k^m 2^k \mathcal{G}(\alpha)$ . Alors

$$L_k + 2^{m+1}R = U \cap 2^k R.$$

*Remarque.* — Puisque  $2^m R \subset U$ , il est toujours possible de choisir pour  $\mathcal{G}(m)$  une base orthogonale de  $R$ , auquel cas  $L_k \supset 2^m R$  si bien que  $L_k = U \cap 2^k R$ .

**2. CODES AFFINES.** — Le lecteur familiarisé avec la théorie des codes correcteurs d'erreur reconnaîtra dans ce que nous appelons « codes affines », les codes de Reed-Muller, ou RM-codes [7].

Mais, pour l'usage que nous en faisons, une présentation purement géométrique de ces « codes » nous a paru préférable, parce que plus simple et moins rebutante pour les non-spécialistes de la théorie des codes — dont nous sommes. Nous n'avons pas trouvé cette présentation dans la littérature ([1], [6], [7], [8]).

**2.1. Notations.** — Soit  $d$  un nombre entier strictement positif. Nous désignons par  $\Omega$  l'ensemble sous-jacent au  $\mathbf{F}_2$ -espace vectoriel  $\mathbf{F}_2^d$ , et par  $n$  le cardinal de  $\Omega$ . On a donc  $n = |\Omega| = 2^d$  <sup>(1)</sup>.

---

(1) Si  $E$  est un ensemble,  $|E|$  désigne son cardinal.

L'ensemble des parties de  $\Omega$  est muni de deux lois :

(a) La « somme des complexes » pour l'addition dans l'espace vectoriel  $\mathbf{F}_2^d$  est notée  $+$  :

$$\text{si } X, Y \subset \Omega, \quad X + Y = \{x + y \mid (x \in X) \text{ et } (y \in Y)\}.$$

(b) La « somme booléenne » ou « différence symétrique » est notée  $\dot{+}$  :

$$\text{si } X, Y \subset \Omega, \quad X \dot{+} Y = \{z \mid (z \in X \cup Y) \text{ et } (z \notin X \cap Y)\}.$$

Nous noterons  $\mathcal{X}(\Omega)$  l'espace vectoriel de dimension  $n = 2^d$  sur  $\mathbf{F}_2$  ainsi défini, muni de la forme bilinéaire suivante :

$$(X, Y) \rightarrow \langle X, Y \rangle = \begin{cases} 0 & \text{si } |X \cap Y| \text{ est pair,} \\ 1 & \text{si } |X \cap Y| \text{ est impair.} \end{cases}$$

Pour cette forme bilinéaire, la base  $\{\{j\} \mid j \in \Omega\}$  de  $\mathcal{X}(\Omega)$  est orthogonale : la forme est donc non dégénérée. Si  $\mathcal{E}$  est un sous-ensemble de  $\mathcal{X}(\Omega)$ , nous désignons par  $\mathcal{E}^0$  son *orthogonal* :

$$\mathcal{E}^0 = \{Y \in \mathcal{X}(\Omega) \mid (\forall X \in \mathcal{E}) (\langle X, Y \rangle = 0)\}.$$

Un code est un sous-espace vectoriel de  $\mathcal{X}(\Omega)$ , soit un sous-ensemble non vide de  $\mathcal{X}(\Omega)$  stable par l'opération différence symétrique. Nous désignons par  $\mathcal{O}(\Omega)$  le code de dimension 1 (droite) engendré par  $\Omega$  :  $\mathcal{O}(\Omega) = \{\emptyset, \Omega\}$ , et par  $\mathcal{H}(\Omega)$  le code orthogonal de  $\mathcal{O}(\Omega)$  ;  $\mathcal{H}(\Omega)$  est l'hyperplan de  $\mathcal{X}(\Omega)$  dont les éléments sont les parties de cardinal pair de  $\Omega$ .

Le groupe des automorphismes de la forme bilinéaire définie plus haut contient un sous-groupe isomorphe à  $\mathfrak{S}(\Omega)$ , groupe des permutations de  $\Omega$ . Une permutation de  $\Omega$  et la transformation linéaire qu'elle définit ainsi dans  $\mathcal{X}(\Omega)$  seront désignées par la même lettre.

Si  $\mathcal{C}$  est un code, le groupe d'automorphismes de  $\mathcal{C}$  est par définition le sous-groupe de  $\mathfrak{S}(\Omega)$  formé des éléments qui laissent globalement fixe  $\mathcal{C}$  ;  $\mathcal{C}$  et  $\mathcal{C}^0$  ont même groupe d'automorphismes.

Soit  $t \in \Omega$  ; la translation de vecteur  $t$  dans  $\mathbf{F}_2^d$  est une permutation de  $\Omega$  et sera notée  $\tau_t$ .

Le groupe des translations est un groupe abélien 2-élémentaire d'ordre  $2^d$  ; il sera noté  $\mathfrak{T}(\Omega)$ .

De même, l'image de  $\text{GL}(\mathbf{F}_2^d)$  dans  $\mathfrak{S}(\Omega)$  sera notée  $\text{GL}(\Omega)$ . Enfin, le produit semi-direct  $\mathfrak{T}(\Omega) \rtimes \text{GL}(\Omega)$  sera noté  $\text{Af}(\Omega)$  (« groupe affine »).

Soit  $X$  une variété affine non-vide de  $\mathbf{F}_2^d$ . L'unique espace vectoriel parallèle à  $X$  et de même dimension sera noté  $\vec{X}$  ; nous dirons que  $\vec{X}$  est l'espace associé à  $X$ .

Si  $\alpha$  est un entier compris entre 0 et  $d$ , soit  $\mathcal{V}_\alpha$  (resp.  $\vec{\mathcal{V}}_\alpha$ ) l'ensemble des variétés affines (resp. sous-espaces vectoriels) de dimension  $\alpha$  de  $\mathbb{F}_2^d$ . On a  $\vec{\mathcal{V}}_\alpha \subset \mathcal{V}_\alpha \subset \mathcal{X}(\Omega)$ . Nous nous proposons d'étudier les codes engendrés par  $\mathcal{V}_\alpha$  et  $\vec{\mathcal{V}}_\alpha$ , notés respectivement  $\langle \mathcal{V}_\alpha \rangle$  et  $\langle \vec{\mathcal{V}}_\alpha \rangle$ , et appelés « codes affines ».

## 2.2. Variétés affines et somme booléenne dans $\mathcal{X}(\Omega)$ .

PROPOSITION I.4. — Soit  $V$  une variété affine non vide de  $\Omega$ , et soit  $\vec{E}$  un sous-espace vectoriel de  $\Omega$ . Alors  $W = \bigcup_{i \in \vec{E}} \tau_i(V)$  est l'unique variété affine contenant  $V$  et dont l'espace associé soit  $\vec{V} + \vec{E}$ .

COROLLAIRE 1. — Soit  $\alpha$  un entier ( $0 \leq \alpha < d$ ). On a

$$[\langle \mathcal{V}_\alpha \rangle, \mathfrak{E}(\Omega)] = \langle \mathcal{V}_{\alpha+1} \rangle,$$

autrement dit  $\langle \mathcal{V}_{\alpha+1} \rangle$  est engendré par l'ensemble des  $X \dot{+} \tau_i(X)$ ,  $X \in \langle \mathcal{V}_\alpha \rangle$ ,  $\tau_i \in \mathfrak{E}(\Omega)$ .

En particulier,  $\langle \mathcal{V}_{\alpha+1} \rangle \subset \langle \mathcal{V}_\alpha \rangle$ , et on peut donc écrire

$$\{\emptyset\} \subset \mathcal{O}(\Omega) = \langle \mathcal{V}_d \rangle \subset \langle \mathcal{V}_{d-1} \rangle \subset \dots \subset \langle \mathcal{V}_1 \rangle = \mathfrak{A}(\Omega) \subset \langle \mathcal{V}_0 \rangle = \mathcal{X}(\Omega).$$

COROLLAIRE 2. — Soit  $\alpha$  un entier ( $0 < \alpha \leq d-1$ ). On a

$$[\langle \mathcal{V}_\alpha \rangle, \text{Af}(\Omega)] = \langle \mathcal{V}_\alpha \rangle,$$

autrement dit  $\langle \mathcal{V}_\alpha \rangle$  est engendré par l'ensemble des

$$X \dot{+} \pi(X), \quad X \in \langle \mathcal{V}_\alpha \rangle, \quad \pi \in \text{Af}(\Omega).$$

COROLLAIRE 3. — Soit  $\alpha$  un entier ( $0 < \alpha \leq d$ ). Alors

$$\langle \vec{\mathcal{V}}_\alpha \rangle = \langle \mathcal{V}_\alpha \rangle.$$

PROPOSITION I.5. — Soient  $\alpha$  et  $\beta$  deux entiers du segment  $[0, d]$ .

(1) Si  $X \in \mathcal{V}_\alpha$  et  $Y \in \mathcal{V}_\beta$ ,  $X \cap Y$  est soit vide, soit une variété affine de dimension au moins égale à  $k(\alpha, \beta) = \sup\{0, \alpha + \beta - d\}$ .

(2) Soit  $X \in \mathcal{V}_\alpha$ . Pour toute variété  $Z$  de  $X$  de dimension  $\gamma \geq k(\alpha, \beta)$  il existe une variété  $Y$  de dimension  $\beta$  telle que  $X \cap Y = Z$ .

Remarques :

(a) D'après le (1) de la proposition I.7, si  $X \in \mathcal{V}_\alpha$  et  $Y \in \mathcal{V}_\beta$  on a

$$|X \cap Y| \equiv 0 \pmod{2^{k(\alpha, \beta)}}.$$

(b) Soit  $X \in \mathcal{V}_\alpha$ . Si  $\gamma$  est un entier inférieur à  $\alpha$ ,  $\mathcal{V}_\gamma(X)$  désigne l'ensemble des sous-variétés de  $X$  de dimension  $\gamma$ . D'autre part, nous appelons « trace » de  $\langle \mathcal{V}_\beta \rangle$  sur  $\mathcal{T}(X)$  l'ensemble  $\{Y \cap X \mid Y \in \langle \mathcal{V}_\beta \rangle\}$ .

Si  $X \in \mathcal{V}_\alpha$ , la trace de  $\langle \mathcal{V}_\beta \rangle$  sur  $\mathcal{T}(X)$  est  $\langle \mathcal{V}_{k(\alpha, \beta)}(X) \rangle$ .

PROPOSITION I.6. — On a

$$\langle \mathcal{V}_{d-1} \rangle = \mathcal{O}(\Omega) \cup \mathcal{V}_{d-1}.$$

2.3. *Dimensions et propriétés combinatoires.* — Nous allons déterminer, pour tout  $\alpha$ , une base de  $\langle \mathcal{V}_\alpha \rangle$ .

LEMME. — Soit  $\{e_i\}_{i \in D}$  une base de  $\mathbf{F}_2^d$ .

Pour tout  $E \subset D$ , désignons par  $\vec{V}_E$  le sous-espace vectoriel de base  $\{e_i\}_{i \in E}$ .

Alors  $\{\vec{V}_E \mid E \in \mathcal{T}(D)\}$  est une base de  $\mathcal{T}(\Omega)$ .

Remarque. — Ce lemme montre essentiellement que si  $D$  est un ensemble fini, la famille  $\{\mathcal{T}(E) \mid E \in \mathcal{T}(D)\}$  forme une base de  $\mathcal{T}(\mathcal{T}(D))$ .

En effet, si  $x = \sum_{i \in E} e_i$ , on a

$$\{x\} = \sum_{F \subset E} \vec{V}_F.$$

THÉORÈME I.4. — Soit  $\alpha$  un entier compris entre 1 et  $d$ .

$$(1) \langle \mathcal{V}_\alpha \rangle^0 = \langle \mathcal{V}_{d+1-\alpha} \rangle;$$

$$(2) \dim \langle \mathcal{V}_\alpha \rangle = \binom{d}{0} + \binom{d}{1} + \dots + \binom{d}{d-\alpha}.$$

Démonstration du théorème I.4. — Pour tout  $\alpha$ , désignons par  $\mathcal{C}_\alpha$  l'espace engendré par  $\{\vec{V}_E \mid (E \subset D) \text{ et } |E| \geq \alpha\}$ .

(a) Du corollaire 1 de la proposition I.4, il résulte que

$$\mathcal{C}_\alpha \subset \langle \mathcal{V}_\alpha \rangle.$$

(b) De la proposition I.5 [remarque (a)], il résulte que

$$\langle \mathcal{V}_{d+1-\alpha} \rangle \subset \langle \mathcal{V}_\alpha \rangle^0, \quad \text{puisque } k(d+1-\alpha, \alpha) = 1.$$

Par suite :

$$\mathcal{C}_{d+1-\alpha} \subset \langle \mathcal{V}_{d+1-\alpha} \rangle \subset \langle \mathcal{V}_\alpha \rangle^0 \subset \mathcal{C}_\alpha^0.$$

(c) Enfin, il résulte du lemme précédent que pour tout  $\alpha$ ,

$$\dim \mathcal{C}_\alpha = \binom{d}{\alpha} + \binom{d}{\alpha+1} + \dots + \binom{d}{d}.$$

On en déduit que

$$\dim \mathcal{C}_{d+1-\alpha} = \binom{d}{d+1-\alpha} + \binom{d}{d+2-\alpha} + \dots + \binom{d}{d},$$

$$\dim \mathcal{C}_\alpha^0 = 2^d - \dim \mathcal{C}_\alpha = 1 + \binom{d}{1} + \dots + \binom{d}{\alpha-1};$$

d'où

$$\dim \mathcal{C}_\alpha^0 = \dim \mathcal{C}_{d+1-\alpha}.$$

Il résulte alors de (b) que

$$\mathcal{C}_{d+1-\alpha} = \langle \mathcal{V}_{d+1-\alpha} \rangle = \langle \mathcal{V}_\alpha \rangle^0 = \mathcal{C}_\alpha^0,$$

d'où

$$\langle \mathcal{V}_\alpha \rangle^0 = \langle \mathcal{V}_{d+1-\alpha} \rangle,$$

$$\dim \langle \mathcal{V}_\alpha \rangle = \binom{d}{\alpha} + \binom{d}{\alpha+1} + \dots + \binom{d}{d}.$$

C. Q. F. D.

Donnons un corollaire de ce théorème qui nous sera utile dans l'étude des réseaux construits à partir des espaces  $\langle \mathcal{V}_\alpha \rangle$ .

**COROLLAIRE.** — Soit  $A \subset \Omega$ , et soit  $k$  un entier tel que  $0 \leq k < d$ . Supposons qu'il existe un entier  $a$ , avec  $k < a \leq d$ , tel que pour tout  $X \in \langle \mathcal{V}_a \rangle$ , on ait  $X \cap A \in \langle \mathcal{V}_{a-k} \rangle$ . Alors  $A \in \langle \mathcal{V}_{d-k} \rangle$ .

*Démonstration du corollaire.* — Pour démontrer que  $A \in \langle \mathcal{V}_{d-k} \rangle$ , nous démontrons que  $A \in \langle \mathcal{V}_{k+1} \rangle^0$ .

Soit donc  $Y \in \mathcal{V}_{k+1}$ . Comme  $k < a$ , il existe  $X \in \mathcal{V}_a$  tel que  $Y \subset X$ . Si  $\vec{X}'$  est un espace supplémentaire de  $\vec{X}$ , soit  $Z$  la variété définie par

$$Z = \bigcup_{t \in \vec{X}'} \tau_t(Y);$$

$Z$  est une variété de dimension  $d - a + k + 1$  (prop. I.4), et  $Z \cap X = Y$ .

Comme par hypothèse  $X \cap A \in \langle \mathcal{V}_{a-k} \rangle = \langle \mathcal{V}_{d-a+k+1} \rangle^0$ , on sait que  $(X \cap A) \cap Z = A \cap (X \cap Z) = A \cap Y$  est de cardinal pair, ce qui achève la démonstration.

**THÉORÈME I.5.** — Soit  $\alpha$  un entier compris entre 0 et  $d$ .

- (1) Pour tout  $X \in \langle \mathcal{V}_\alpha \rangle$ ,  $X \neq O$ , on a  $|X| \geq 2^\alpha$ .
- (2) Si  $X \in \langle \mathcal{V}_\alpha \rangle$ , pour que  $|X| = 2^\alpha$  il faut et il suffit que  $X \in \langle \mathcal{V}_\alpha \rangle$ .

*Démonstration du théorème I.5.* — Les assertions (1) et (2) étant manifestement vraies pour  $\alpha = d$ , et aussi pour  $\alpha = d - 1$  (proposition I.6) nous raisonnons par *récurrence descendante* sur  $\alpha$  :

Supposons que (1) et (2) soient vérifiées pour  $\alpha + 1$  ( $\alpha \leq d - 2$ ), et montrons qu'elles le sont pour  $\alpha$  :

1° Soit  $X \in \langle \mathcal{V}_\alpha \rangle$ . Démontrons que  $|X| \geq 2^\alpha$ .

(a) Si  $X \in \langle \mathcal{V}_{\alpha+1} \rangle$ , d'après l'hypothèse de récurrence on a  $|X| \geq 2^{\alpha+1}$ .

(b) Supposons donc  $X \in \langle \mathcal{V}_\alpha \rangle$ ,  $X \notin \langle \mathcal{V}_{\alpha+1} \rangle$ . On a :

$$\langle \mathcal{V}_{\alpha+1} \rangle = \langle \mathcal{V}_{d-\alpha} \rangle^0.$$

Par conséquent, il existe une variété  $V \in \mathcal{V}_{d-\alpha}$  telle que  $|V \cap X| \equiv 1 \pmod{2}$ .

Si  $V' \in \mathcal{V}_{d-\alpha}$  est une variété parallèle à  $V$ , on sait que

$$V \dot{+} V' = V \cup V' \in \mathcal{V}_{d-\alpha+1}.$$

Or  $X \in \langle \mathcal{V}_\alpha \rangle = \langle \mathcal{V}_{d-\alpha+1} \rangle^0$ . On en déduit que, pour toute variété  $V'$  parallèle à  $V$ , on a

$$|V' \cap X| \equiv 1 \pmod{2}.$$

Il résulte de ce raisonnement que  $X$  a au moins un point dans chaque parallèle à  $V$ . Comme il y a  $2^\alpha$  parallèles distinctes à  $V$ , deux à deux disjointes, on voit que  $|X| \geq 2^\alpha$ .

2° Démontrons alors que  $\mathcal{V}_\alpha = \{X \in \langle \mathcal{V}_\alpha \rangle \mid |X| = 2^\alpha\}$ .

Le raisonnement de (1) nous montre que si  $X \in \langle \mathcal{V}_\alpha \rangle$  et  $|X| = 2^\alpha$ , il existe  $\vec{V} \in \vec{\mathcal{V}}_{d-\alpha}$  tel que  $X$  ait un point et un seul dans toute variété d'espace associé  $\vec{V}$ . Quitte à composer par une translation, on peut toujours supposer que  $X \cap \vec{V} = \{0\}$ . Ainsi, nous devons démontrer que  $X$  est un espace vectoriel.

(a) Soit  $t \in \vec{V}$ ,  $t \neq 0$  : Montrons que  $X \cup \tau_t(X) \in \mathcal{V}_{\alpha+1}$ .

Puisque  $X$  a un point et un seul dans toute variété d'espace associé  $\vec{V}$ , et que chacune de ces variétés est stable par  $\tau_t$ , il est clair que  $X \cap \tau_t(X) = \emptyset$ , donc que

$$|X \dot{+} \tau_t(X)| = |X \cup \tau_t(X)| = |X| + |\tau_t(X)| = 2^{\alpha+1}.$$

D'après l'hypothèse de récurrence, pour démontrer que  $X \cup \tau_t(X) \in \mathcal{V}_{\alpha+1}$ , il nous suffit de démontrer que  $X \cup \tau_t(X) \in \langle \mathcal{V}_{\alpha+1} \rangle$ . Or comme  $X \in \langle \mathcal{V}_\alpha \rangle$  cela résulte du corollaire 1 de la proposition I.4.

(b) Nous pouvons alors démontrer que  $X$  est un sous-espace vectoriel.

Pour cela, puisque  $X$  contient 0, il suffit de montrer que si  $u$  et  $v$  sont deux points distincts de  $X$ ,  $(u + v)$  est aussi dans  $X$ .

Cela revient donc à montrer que si  $X$  contient trois points d'un plan vectoriel, il contient le quatrième.

Soit  $\vec{P}$  un plan vectoriel, dont  $X$  contient au moins trois points. Comme pour  $t \in \vec{V}$ ,  $t \neq 0$ ,  $X + \tau_t(X) = X \cup \tau_t(X)$  est un espace vectoriel, on a évidemment  $\vec{P} \subset X + \tau_t(X)$ .

On constate alors que  $k(\alpha + 1, d - \alpha + 1) = 2$ , et en appliquant la proposition I.5 (2) on voit qu'il existe  $V \in \mathcal{V}_{d-\alpha+1}$  tel que

$$V \cap (X + \tau_t(X)) = \vec{P}.$$

Mais  $X$  est orthogonal à  $V$ , puisque  $X \in \langle \mathcal{V}_\alpha \rangle$ .

Comme  $|V \cap X| \geq 3$  par hypothèse, on a donc  $V \cap X = \vec{P}$  et  $\vec{P} \subset X$ .

#### 2.4. Groupes d'automorphismes.

THÉORÈME I.6. — *Le groupe d'automorphismes du code  $\langle \mathcal{V}_\alpha \rangle$  est :*

$\mathfrak{H}(\Omega)$  si  $\alpha = 0, 1, d$ ;

$\text{Af}(\Omega)$  pour  $2 \leq \alpha \leq d - 1$ .

*Démonstration du théorème I.6 :*

1° Il est évident que

$$\langle \mathcal{V}_0 \rangle = \mathcal{X}(\Omega), \quad \langle \mathcal{V}_1 \rangle = \mathcal{H}(\Omega) \quad \text{et} \quad \langle \mathcal{V}_d \rangle = \mathcal{O}(\Omega).$$

Le groupe d'automorphismes de chacun de ces trois codes est donc bien  $\mathfrak{H}(\Omega)$ .

2° Soit  $\alpha$  compris entre 2 et  $d - 1$ .

(a) Il est clair que  $\text{Af}(\Omega)$  fixe globalement  $\mathcal{V}_\alpha$ , donc est contenu dans  $\text{Aut}(\langle \mathcal{V}_\alpha \rangle)$ .

(b) Soit réciproquement  $\sigma \in \text{Aut}(\langle \mathcal{V}_\alpha \rangle)$ . On peut supposer que  $\sigma(0) = 0$ ; nous allons alors démontrer que  $\sigma \in \text{GL}(\Omega)$ .

Pour cela, il nous suffit de démontrer que l'image d'un plan par  $\sigma$  est encore un plan.

Quitte à remplacer  $\langle \mathcal{V}_\alpha \rangle$  par  $\langle \mathcal{V}_\alpha \rangle^0 = \langle \mathcal{V}_{d+1-\alpha} \rangle$ , on peut supposer que  $2\alpha \leq d + 1$ . Comme  $\mathcal{V}_\alpha = \{X \in \langle \mathcal{V}_\alpha \rangle \mid |X| = 2^\alpha\}$ ,  $\sigma$  opère sur  $\langle \mathcal{V}_\alpha \rangle$ .

Par suite  $\sigma$  opère sur l'ensemble

$$\{V \cap V' \mid V, V' \in \mathcal{V}_\alpha, |V \cap V'| = 4\}.$$

Cet ensemble est égal à  $\mathcal{V}_2$ , puisque

$$k(\alpha, \alpha) = \sup \{0, 2\alpha - d\} \leq 1 \quad (\text{proposition I.5}).$$

Nous allons mettre en évidence dans  $\text{Af}(\Omega)$  des *involutions* particulières, que nous utiliserons par la suite.

Soit  $H \subset \Omega$  un hyperplan, et soit  $t \in \vec{H}$ .

Désignons par  $\sigma(H; t)$  la permutation de  $\Omega$  définie comme suit :  $\sigma(H; t)$  induit l'identité sur  $\Omega \setminus H$ ,  $\sigma(H; t)$  opère sur  $H$  comme  $\tau_t$ .

PROPOSITION I.9. — Pour tout  $H \in \mathcal{V}_{d-1}$  et tout  $t \in \vec{H}$ ,  $\sigma(H; t) \in \text{Af}(\Omega)$ .

Démonstration de la proposition I.9. — Il est facile de vérifier que si  $\pi \in \text{Af}(\Omega)$  et si  $\vec{\pi}$  est sa composante sur  $\text{GL}(\Omega)$ , alors

$$\pi \circ \sigma(H; t) \circ \pi^{-1} = \sigma(\pi(H); \vec{\pi}(t)).$$

Quitte à conjuguer  $\sigma(H; t)$  par une translation non parallèle à  $H$ , on peut donc supposer que  $H$  ne contient pas 0 :  $H \not\subset \vec{H}$ . Désignons alors par  $\mu_H$  la forme linéaire non nulle de noyau  $\vec{H}$ .

On voit que  $\sigma(H; t)$  n'est autre que la transvection déterminée par la formule

$$\sigma(H; t)(x) = x + \mu_H(x) \cdot t \quad \text{pour } x \in \Omega.$$

## CHAPITRE II

### UNE FAMILLE INFINIE DE RÉSEAUX ET LEURS GROUPES D'AUTOMORPHISMES

Nous reprenons les notations du paragraphe 2.

L'entier  $d$  est maintenant supposé au moins égal à 4.

Désignons par  $m$  la partie entière de  $\frac{d}{2}$ .

Soit  $\{v_i\}_{i \in \Omega}$  une base orthogonale de  $\mathbb{Q}^n$ , telle que, pour tout  $i$  dans  $\Omega$ ,  $v_i \cdot v_i = 2^{-m}$ .

Nous désignons par  $R$  le réseau  $2^m$ -modulaire trivial

$$R = \bigoplus \mathbb{Z} \cdot v_i.$$

Si  $X \subset \Omega$ , posons

$$v_K = \sum_{i \in X} v_i.$$

Si  $S \subset \Omega$ , désignons par  $\varepsilon_S$  la transformation orthogonale de  $\mathbb{Q}^n$  définie par

$$\begin{aligned} \varepsilon_S(v_i) &= -v_i & \text{si } i \in S, \\ \varepsilon_S(v_i) &= v_i & \text{si } i \notin S. \end{aligned}$$

L'application  $S \rightarrow \varepsilon_S$  définit un homomorphisme injectif de groupes entre  $\mathcal{T}(\Omega)$  muni de la loi  $\dagger$  et  $\text{GL}(\mathbb{Q}^n)$ . Pour tout code  $\mathcal{C}$  dans  $\mathcal{T}(\Omega)$ , nous désignons par  $E(\mathcal{C})$  le groupe des  $\varepsilon_S$  ( $S \in \mathcal{C}$ ).

Enfin, par abus de notations, si  $\pi \in \mathfrak{S}(\Omega)$  nous désignons encore par  $\pi$  la transformation orthogonale de  $\mathbb{Q}^n$  définie par

$$\pi(v_i) = v_{\pi(i)} \quad \text{pour tout } i \in \Omega.$$

On considère ainsi  $\mathfrak{S}(\Omega)$  comme un sous-groupe de  $\text{GL}(\mathbb{Q}^n)$ . Si  $X \subset \Omega$ , et si  $\pi \in \mathfrak{S}(\Omega)$ , on a

$$\pi(v_X) = v_{\pi(X)}.$$

$\mathfrak{S}(\Omega)$  normalise  $E(\mathcal{T}(\Omega))$ , puisque

$$\pi \cdot \varepsilon_S \cdot \pi^{-1} = \varepsilon_{\pi(S)} \quad \text{pour tous } \pi \in \mathfrak{S}(\Omega) \text{ et } S \subset \Omega.$$

On a donc

$$\text{Aut } R = E(\mathcal{T}(\Omega)) \rtimes \mathfrak{S}(\Omega) \quad (\text{proposition I.2}).$$

1. LE RÉSEAU  $U$  ET SON DUAL. — Nous désignons par  $U$  le sous- $\mathbf{Z}$ -module de  $\mathbb{Q}^n$  engendré par

$$\mathcal{G} = \{ 2^\alpha v_{X_\alpha} \mid (X_\alpha \in \mathcal{V}_{2m-2\alpha}) (0 \leq \alpha \leq m) \}.$$

THÉORÈME II.1 :

(1)  $U$  est un réseau, et  $2^m R \subset U \subset U^0 \subset R$ .

(2)  $U^0$  est le sous- $\mathbf{Z}$ -module engendré par

$$\mathcal{G}' = \{ 2^\alpha v_{X'_\alpha} \mid (X'_\alpha \in \mathcal{V}_{d-1-2\alpha}) (0 \leq \alpha < m) \} \cup \{ 2^m v_i \mid i \in \Omega \}.$$

(3) Pour  $0 \leq \alpha \leq m$ ,  $\bar{U}_\alpha(R) = \langle \mathcal{V}_{2m-2\alpha} \rangle$ .

Pour  $0 \leq \alpha < m$ ,  $\bar{U}_\alpha^0(R) = \langle \mathcal{V}_{d-1-2\alpha} \rangle$ .

Démonstration du théorème II.1 :

1° Désignons provisoirement par  $U'$  le réseau engendré par l'ensemble  $\mathcal{G}'$ . En utilisant essentiellement la proposition I.5, on vérifie que

$$2^m R \subset U \subset U' \subset U^0 \subset R.$$

2° Démontrons la troisième assertion du théorème.

D'après la définition de  $U$ , il est clair que

$$\bar{U}_\alpha(R) \supset \langle \mathcal{V}_{2m-2\alpha} \rangle \quad \text{pour } 0 \leq \alpha \leq m.$$

En considérant les codes orthogonaux, on en déduit donc [théorème I.2(1) et théorème I.4] :

$$U_{m-1-\alpha}^0(R) \subset \langle \mathcal{V}_{d+1-2m+2\alpha} \rangle.$$

Or il résulte de 1° que

$$\bar{U}_{m-1-\alpha}^0(R) \supset \langle \mathcal{V}_{d+1-2m+2\alpha} \rangle.$$

On en déduit donc que

$$\bar{U}_{m-1-\alpha}^0(R) = \langle \mathcal{V}_{d+1-2m+2\alpha} \rangle$$

et par orthogonalité :

$$\bar{U}_{\alpha}(R) = \langle \mathcal{V}_{2m-2\alpha} \rangle.$$

3° On a

$$2^m R \subset U^0 \subset R, \quad \bar{U}_{\alpha}^0(R) = \langle \mathcal{V}_{d-1-2\alpha} \rangle$$

et

$$2^{\alpha} v_{X'_\alpha} \in U^0 \quad \text{pour} \quad X'_\alpha \in \mathcal{V}_{d-1-2\alpha}.$$

D'après le corollaire 2 du théorème I.3,  $U^0$  est engendré modulo  $2^m R$  par  $\{2^{\alpha} v_{X'_\alpha} \mid (X'_\alpha \in \mathcal{V}_{d-1-2\alpha}) \ (0 \leq \alpha < m)\}$ , ce qui démontre la *deuxième assertion du théorème*.

*Remarque.* — Il est facile de vérifier, en calculant le carré scalaire des générateurs, que le réseau  $U$  est pair.

Le théorème II.1 montre que, pour  $d$  impair, le réseau  $U$  est un réseau unimodulaire pair de  $\mathbf{Q}^{2^d}$ .

2. PETITS VECTEURS ET CHANGEMENTS DE SIGNES. — Si  $L$  est un réseau de  $\mathbf{Q}^n$ , nous appelons « *petits vecteurs* » de  $L$  les vecteurs non nuls de  $L$  de carré scalaire minimal.

Désignons par  $G$  le groupe d'automorphismes de  $U$  et posons alors

$$E = E(\mathcal{P}(\Omega)) \cap G.$$

THÉORÈME II.2 :

(1) Les petits vecteurs de  $U$  ont pour carré scalaire  $2^m$ , et ce sont les vecteurs

$$\varepsilon_S(2^{\alpha} v_{X_\alpha}) \quad \text{pour} \quad 0 \leq \alpha < m,$$

avec

$$X_\alpha \in \mathcal{V}_{2m-2\alpha}, \quad S \subset X_\alpha \quad \text{et} \quad S \in \langle \mathcal{V}_{2m-2\alpha-2} \rangle,$$

ainsi que les  $\pm 2^m v_i \ (i \in \Omega)$ .

Si  $d$  est pair, les petits vecteurs de  $U^0$  ont pour carré scalaire  $2^{m-1}$ , et ce sont les vecteurs

$$\varepsilon_S(2^{\alpha} v_{X'_\alpha}) \quad \text{pour} \quad 0 \leq \alpha < m,$$

avec

$$X'_\alpha \in \mathcal{V}_{d-1-2\alpha}, \quad S \subset X'_\alpha \quad \text{et} \quad S \in \langle \mathcal{V}_{d-1-2\alpha-2} \rangle.$$

(2)  $E = E(\langle \mathcal{V}_{d-2} \rangle)$ .

*Démonstration du théorème II.2 :*

1° *Démontrons que*  $E \supset E(\langle \mathcal{V}_{d-2} \rangle)$ .

Pour cela, puisque  $X \rightarrow \varepsilon_X$  est un homomorphisme de groupes, il nous suffit de démontrer que si  $X \in \mathcal{V}_{d-2}$ , les images par  $\varepsilon_X$  des générateurs de  $U$  sont encore dans  $U$  : on en déduira en effet que  $\varepsilon_X(U) \subset U$ , donc que  $\varepsilon_X \in G$  (cf. I.1).

Si  $X_\alpha \in \mathcal{V}_{2m-2\alpha}$  ( $0 \leq \alpha \leq m$ ) et si  $X \in \mathcal{V}_{d-2}$ ,

$$\varepsilon_X(2^\alpha v_{X_\alpha}) = 2^\alpha v_{X_\alpha} - 2^{\alpha+1} v_{X_\alpha \cap X}.$$

On sait [prop. I.7 (1)] que  $X \cap X_\alpha$  est soit vide, soit une variété affine de dimension au moins égale à

$$k(2m - 2\alpha, d - 2) = \sup \{ 0, 2m - 2\alpha - 2 \}, \quad \text{donc} \quad 2^{\alpha+1} v_{X \cap X_\alpha} \in U$$

d'après la proposition I.4.

Ceci prouve bien que  $\varepsilon_X(2^\alpha v_{X_\alpha}) \in U$ .

2° *Forme des petits vecteurs* : Soit  $x$  un vecteur de  $U$  (resp. de  $U^0$ ).

Soit  $\alpha$  l'entier ( $0 \leq \alpha \leq m$ ) tel que  $x \in 2^\alpha R$  et  $x \notin 2^{\alpha+1} R$ .

Posons  $x = 2^\alpha y$ .

D'après le théorème II.1 (3), on peut écrire

$$y = v_{X_\alpha} + 2z, \quad \text{où} \quad X_\alpha \in \langle \mathcal{V}_{2m-2\alpha} \rangle$$

(resp.  $y = y_{X'_\alpha} + 2z$ , où  $X'_\alpha \in \langle \mathcal{V}_{d-1-2\alpha} \rangle$ ) et  $z \in R$ , soit encore  $y = \sum_{i \in \Omega} y_i v_i$ ,

où  $y_i$  est impair si  $i \in X_\alpha$  (resp.  $i \in X'_\alpha$ ) et pair si  $i \notin X_\alpha$  (resp.  $i \notin X'_\alpha$ ). On voit alors que  $y$  est de carré scalaire minimal si  $X_\alpha$  (resp.  $X'_\alpha$ ) est de cardinal minimal, et si  $y_i = \pm 1$  pour  $i \in X_\alpha$  (resp.  $i \in X'_\alpha$ ), et  $y_i = 0$  pour  $i \notin X_\alpha$  (resp.  $i \notin X'_\alpha$ ). Grâce au théorème I.5, on peut alors conclure que les vecteurs de

$$(U \cap 2^\alpha R) - (U \cap 2^{\alpha+1} R) \quad [\text{resp. } (U^0 \cap 2^\alpha R) - (U^0 \cap 2^{\alpha+1} R)]$$

de carré scalaire minimal sont de la forme  $\varepsilon_S(2^\alpha v_{X_\alpha})$ , avec  $X_\alpha \in \mathcal{V}_{2m-2\alpha}$  et  $S \subset X_\alpha$  [resp.  $\varepsilon_S(2^\alpha v_{X'_\alpha})$ , avec  $X'_\alpha \in \mathcal{V}_{d-1-2\alpha}$  et  $S \subset X'_\alpha$ ].

Un calcul facile montre que ces vecteurs sont tous de carré scalaire  $2^m$  pour  $0 \leq \alpha \leq m$  (resp. de carré scalaire  $2^{m-1}$  pour  $0 \leq \alpha < m$ ).

Remarquons d'autre part que

$$\varepsilon_S(2^\alpha v_{X_\alpha}) = 2^\alpha v_{X_\alpha} - 2^{\alpha+1} v_S \quad \text{si } S \subset X_\alpha \quad [\text{resp. } \varepsilon_S(2^\alpha v_{X'_\alpha}) = 2^\alpha v_{X'_\alpha} - 2^{\alpha+1} v_S \text{ si } S \subset X'_\alpha].$$

Par conséquent si  $X_\alpha \in \mathcal{V}_{2m-2\alpha}$  et si  $\varepsilon_S(2^\alpha v_{X_\alpha}) \in U$  [resp.  $X'_\alpha \in \mathcal{V}_{d-1-2\alpha}$  et  $\varepsilon_S(2^\alpha v_{X'_\alpha}) \in U^0$ ], pour  $0 \leq \alpha < m$  on a  $S \in \langle \mathcal{V}_{2m-2\alpha-2} \rangle$  (resp.  $S \in \langle \mathcal{V}_{d-1-2\alpha-2} \rangle$ ) d'après le théorème II.1 (3).

3° *Petits vecteurs* : Nous pouvons démontrer à présent que tous ces  $\varepsilon_S(2^\alpha v_{X_\alpha})$ , avec  $0 \leq \alpha < m$ ,  $X_\alpha \in \mathcal{V}_{2m-2\alpha}$ ,  $S \subset X_\alpha$  et  $S \in \langle \mathcal{V}_{2m-2\alpha-2} \rangle$  [resp.  $\varepsilon_S(2^\alpha v_{X'_\alpha})$  avec  $0 \leq \alpha < m$ ,  $X'_\alpha \in \mathcal{V}_{d-1-2\alpha}$ ,  $S \subset X'_\alpha$  et  $S \in \langle \mathcal{V}_{d-1-2\alpha-2} \rangle$ ] appartiennent à  $U$  (resp. à  $U^0$ ), ce qui achèvera la démonstration de la première assertion du théorème II.2.

D'après la remarque (b) qui suit la proposition I.5, on sait que si  $S \subset S_\alpha$  et si  $S \in \langle \mathcal{V}_{2m-2\alpha-2} \rangle$  (resp. si  $S \subset X'_\alpha$  et si  $S \in \langle \mathcal{V}_{d-1-2\alpha-2} \rangle$ ) il existe  $X \in \langle \mathcal{V}_{d-2} \rangle$  tel que  $X \cap X_\alpha = S$  (resp.  $X \cap X'_\alpha = S$ ). On a alors :

$$\varepsilon_X(2^\alpha v_{X_\alpha}) = \varepsilon_S(2^\alpha v_{X_\alpha}) \in U$$

puisque  $\varepsilon_X \in E$  d'après 1° [resp.  $\varepsilon_X(2^\alpha v_{X'_\alpha}) = \varepsilon_S(2^\alpha v_{X'_\alpha}) \in U^0$  puisque  $\varepsilon_X \in E$  d'après 1°]. Ceci démontre la première assertion du théorème.

4° *Groupe E* : Soit  $X \subset \Omega$  tel que  $\varepsilon_X \in G$ . Nous allons démontrer que  $X \in \langle \mathcal{V}_{d-2} \rangle$ . Pour tout  $\alpha$  ( $0 \leq \alpha < m$ ) et tout  $X_\alpha \in \mathcal{V}_{2m-2\alpha}$ , on a

$$\varepsilon_X(2^\alpha v_{X_\alpha}) = 2^\alpha v_{X_\alpha} - 2^{\alpha+1} v_{X \cap X_\alpha} \in U, \quad \text{donc } X \cap X_\alpha \in \langle \mathcal{V}_{2m-2\alpha-2} \rangle.$$

Cette propriété est vérifiée en particulier pour  $\alpha = 0$ ; pour démontrer que  $X \in \langle \mathcal{V}_{d-2} \rangle$ , appliquons le corollaire du théorème I.4 avec  $k = 2$  et  $a = 2m$  : On a bien  $k < a$  puisque  $m \geq 2$ .

Si  $k$  et  $l$  sont deux entiers,  $k \leq l$ , désignons par  $\nu(k, l)$  le nombre de sous-espaces vectoriels de dimension  $k$  dans un  $\mathbf{F}_2$ -espace vectoriel de dimension  $l$ . Alors :

COROLLAIRE 1. — *Le nombre des petits vecteurs de  $U$  est*

$$\delta = 2^{d+1} \sum_{\alpha=0}^{\alpha=m} 2^{\binom{2m-2\alpha}{2}} \nu(2m-2\alpha, d).$$

*Le nombre des petits vecteurs de  $U^0$  est, pour  $d$  pair :*

$$\delta' = 2^{d+1} \sum_{\alpha=0}^{\alpha=m-1} 2^{\binom{d-1-2\alpha}{2}} \nu(d-1-2\alpha, d).$$

C'est une conséquence du théorème précédent et du théorème I.4.

Posons, pour  $0 \leq \alpha \leq m$  :

$$\begin{aligned} P_\alpha &= \{ \varepsilon_X(2^\alpha v_{X_\alpha}) \mid (X \in \langle \mathcal{V}_{d-2} \rangle) (X_\alpha \in \mathcal{V}_{2m-2\alpha}) \}, \\ \vec{P}_\alpha &= \{ \varepsilon_X(2^\alpha v_{X'_\alpha}) \mid (X \in \langle \mathcal{V}_{d-2} \rangle) (\vec{X}_\alpha \in \vec{\mathcal{V}}_{2m-2\alpha}) \} \end{aligned}$$

et aussi, pour  $0 \leq \alpha < m$  :

$$\begin{aligned} P'_\alpha &= \{ \varepsilon_X (2^\alpha v_{X'_\alpha}) \mid (X \in \langle \mathcal{V}_{d-2} \rangle) (X'_\alpha \in \mathcal{V}_{d-1-2\alpha}) \}, \\ \vec{P}'_\alpha &= \{ \varepsilon_X (2^\alpha v_{\vec{X}'_\alpha}) \mid (X \in \langle \mathcal{V}_{d-2} \rangle) (\vec{X}'_\alpha \in \vec{\mathcal{V}}_{d-1-2\alpha}) \}. \end{aligned}$$

Alors :

COROLLAIRE 2. — Pour  $0 \leq \alpha < m$  :

$U \cap 2^\alpha R$  est engendré par  $\vec{P}_\alpha$ ;

$U^0 \cap 2^\alpha R$  est engendré par  $\vec{P}'_\alpha$ .

*Démonstration du corollaire 2.* — Soit  $\alpha$  tel que  $0 \leq \alpha < m$ . Désignons par  $\langle \vec{P}_\alpha \rangle$  (resp.  $\langle \vec{P}'_\alpha \rangle$ ) le groupe engendré par  $\vec{P}_\alpha$  (resp.  $\vec{P}'_\alpha$ ). Il est clair que  $\langle \vec{P}_\alpha \rangle \subset U \cap 2^\alpha R$  (resp.  $\langle \vec{P}'_\alpha \rangle \subset U^0 \cap 2^\alpha R$ ). On sait que (corollaire 2 du théorème I.3)  $U \cap 2^\alpha R$  (resp.  $U^0 \cap 2^\alpha R$ ) est engendré par

$$\bigcup_{\beta=\alpha}^{\beta=m} \{ 2^\beta v_{X_\beta} \mid X_\beta \in \mathcal{V}_{2m-2\beta} \} \quad \left( \text{resp. par } \bigcup_{\beta=\alpha}^{\beta=m-1} \{ 2^\beta v_{X'_\beta} \mid X'_\beta \in \mathcal{V}_{d-1-2\beta} \} \cup \{ 2^m v_i \mid i \in \Omega \} \right).$$

Démontrons donc, par récurrence sur  $\beta$ , que pour  $\alpha \leq \beta \leq m$ ,  $2^\beta v_{X_\beta} \in \langle \vec{P}_\alpha \rangle$  (resp. pour  $\alpha \leq \beta < m$ ,  $2^\beta v_{X'_\beta} \in \langle \vec{P}'_\alpha \rangle$  et  $2^m v_i \in \langle \vec{P}_\alpha \rangle$ ).

(a) L'assertion est vraie pour  $\beta = \alpha$ . En effet, si  $X_\alpha \in \mathcal{V}_{2m-2\alpha}$ ,  $X_\alpha \notin \vec{\mathcal{V}}_{2m-2\alpha}$  (resp.  $X'_\alpha \in \mathcal{V}_{d-1-2\alpha}$ ,  $X'_\alpha \notin \vec{\mathcal{V}}_{d-1-2\alpha}$ ), il existe (puisque  $\alpha < m$ ),  $\vec{Y}_\alpha$  et  $\vec{Z}_\alpha$  dans  $\vec{\mathcal{V}}_{2m-2\alpha}$  tels que  $X_\alpha = \vec{Y}_\alpha + \vec{Z}_\alpha$  (resp.  $\vec{Y}'_\alpha$  et  $\vec{Z}'_\alpha$  dans  $\vec{\mathcal{V}}_{d-1-2\alpha}$  tels que  $X'_\alpha = \vec{Y}'_\alpha + \vec{Z}'_\alpha$ ).

On a alors

$$2^\alpha v_{X_\alpha} = 2^\alpha v_{\vec{Y}_\alpha} + \varepsilon_{\vec{Y}_\alpha \cap \vec{Z}_\alpha} (2^\alpha v_{\vec{Z}_\alpha}) \quad [\text{resp. } 2^\alpha v_{X'_\alpha} = 2^\alpha v_{\vec{Y}'_\alpha} + \varepsilon_{\vec{Y}'_\alpha \cap \vec{Z}'_\alpha} (2^\alpha v_{\vec{Z}'_\alpha})];$$

donc  $2^\alpha v_{X_\alpha} \in \langle \vec{P}_\alpha \rangle$  (resp.  $2^\alpha v_{X'_\alpha} \in \langle \vec{P}'_\alpha \rangle$ ).

(b) Supposons la propriété démontrée pour  $\beta$ , et démontrons-la pour  $\beta + 1$ , pour  $\beta \leq m - 1$  (resp.  $\beta < m - 1$ ).

Soit  $X_{\beta+1} \in \mathcal{V}_{2m-2(\beta+1)}$  (resp.  $X'_{\beta+1} \in \mathcal{V}_{d-1-2(\beta+1)}$ ).

Il existe  $X_\beta \in \mathcal{V}_{2m-2\beta}$  (resp.  $X'_\beta \in \mathcal{V}_{d-1-2\beta}$ ) et  $X \in \mathcal{V}_{d-2}$  tels que  $X_{\beta+1} = X \cap X_\beta$  (resp.  $X'_{\beta+1} = X \cap X'_\beta$ ) [proposition I.5 (2)]. Par l'hypothèse de récurrence, on sait que  $2^\beta v_{X_\beta} \in \langle \vec{P}_\alpha \rangle$  (resp.  $2^\beta v_{X'_\beta} \in \langle \vec{P}'_\alpha \rangle$ ).

De plus, le groupe  $E$  opère évidemment sur  $\langle \vec{P}_\alpha \rangle$  (resp.  $\langle \vec{P}'_\alpha \rangle$ ), puisque ce groupe laisse globalement invariant l'ensemble  $\vec{P}_\alpha$  (resp.  $\vec{P}'_\alpha$ ).

Donc

$$\varepsilon_X(2^\beta v_{X_\beta}) = 2^\beta v_{X_\beta} - 2^{\beta+1} v_{X_{\beta+1}} \in \langle \vec{P}_\alpha \rangle$$

et par suite :

$$2^{\beta+1} v_{X_{\beta+1}} \in \langle \vec{P}_\alpha \rangle$$

$$\left[ \text{resp. } \varepsilon_X(2^\beta v_{X'_\beta}) = 2^\beta v_{X'_\beta} - 2^{\beta+1} v_{X'_{\beta+1}} \in \langle \vec{P}'_\alpha \rangle, \text{ d'où } 2^{\beta+1} v_{X'_{\beta+1}} \in \langle \vec{P}'_\alpha \rangle \right].$$

Il nous reste à établir dans le cas où  $d$  est pair que, pour  $i \in \Omega$ ,  $2^m v_i \in \langle \vec{P}'_\alpha \rangle$ .

D'après la récurrence qui précède, nous savons que

$$\varepsilon_X(2^{m-1}(v_i + v_j)) \in \langle \vec{P}'_\alpha \rangle \quad \text{pour } X \in \langle \mathcal{V}_{d-2} \rangle \quad (i, j \in \Omega; i \neq j).$$

On en déduit que  $2^{m-1}(v_i - v_j) \in \langle \vec{P}'_\alpha \rangle$  pour  $i, j \in \Omega$ ,  $i \neq j$ ; d'où

$$2^m v_i = 2^{m-1}(v_i + v_j) + 2^{m-1}(v_i - v_j) \in \langle \vec{P}'_\alpha \rangle.$$

C. Q. F. D.

3. LE GROUPE N. — Désignons par N l'intersection du groupe d'automorphismes de R et du groupe d'automorphismes de U : N est le sous-groupe du groupe  $E(\mathcal{A}(\Omega)) \rtimes \mathfrak{S}(\Omega)$  qui conserve globalement U.

Désignons par E le groupe  $E(\langle \mathcal{V}_{d-2} \rangle)$ .

THÉORÈME II.3 :

(1) Le groupe N est égal au produit semi-direct  $E \rtimes \text{Af}(\Omega)$ .

(2) Les orbites de N sur l'ensemble des petits vecteurs de U sont les ensembles  $P_\alpha$  ( $0 \leq \alpha \leq m$ ).

Si  $d$  est pair, les orbites de N sur l'ensemble des petits vecteurs de  $U^0$  sont les ensembles  $P'_\alpha$  ( $0 \leq \alpha < m$ ).

Démonstration du théorème II.3 :

1° (a) Si  $\pi \in \text{Af}(\Omega)$  et  $X_\alpha \in \mathcal{V}_{2m-2\alpha}$ , on a

$$\pi(2^\alpha v_{X_\alpha}) = 2^\alpha v_{\pi(X_\alpha)},$$

et il est donc évident que  $\text{Af}(\Omega) \subset N$ .

D'après le théorème II.2, et puisque  $\text{Af}(\Omega)$  normalise E, on a

$$E \rtimes \text{Af}(\Omega) \subset N.$$

(b) Soient réciproquement  $\pi \in \mathfrak{S}(\Omega)$  et  $X \subset \Omega$  tels que  $\varepsilon_X \cdot \pi \in N$ . On a

$$\varepsilon_X \pi(2^\alpha v_{X_\alpha}) = \varepsilon_X(2^\alpha v_{\pi(X_\alpha)}),$$

et par conséquent, pour toute variété  $X_\alpha \in \mathfrak{V}_{2m-2\alpha}$ ,  $\pi(X_\alpha) \in \langle \mathfrak{V}_{2m-2\alpha} \rangle$ . Comme  $m \geq 2$ , on a  $2 \leq 2m-2 \leq d-1$ ; en prenant  $\alpha = 1$ , on voit que  $\pi$  est dans le groupe d'automorphismes de  $\langle \mathfrak{V}_{2m-2} \rangle$ , et il résulte alors du théorème I.6 que  $\pi \in \text{Af}(\Omega)$ . Comme en particulier  $\pi \in N$ , on en déduit  $\varepsilon_X = (\varepsilon_X \pi) \pi^{-1} \in N$ , donc  $\varepsilon_X \in E$  et  $X \in \langle \mathfrak{V}_{d-2} \rangle$  d'après le théorème II.2. En conclusion, nous avons bien démontré que

$$\varepsilon_X \cdot \pi \in E(\langle \mathfrak{V}_{d-2} \rangle) \rtimes \text{Af}(\Omega).$$

2° Comme  $\text{Af}(\Omega)$  est transitif sur tout  $\mathfrak{V}_a$  ( $0 \leq a \leq d$ ), il est évident que les orbites de  $N$  sur l'ensemble des petits vecteurs de  $U$  (resp., si  $d$  est pair, de  $U^0$ ) sont les ensembles  $P_\alpha$  ( $0 \leq \alpha \leq m$ ) (resp.  $P'_\alpha$  pour  $0 \leq \alpha \leq m$ ); cela résulte en effet de la formule

$$(\varepsilon_X \cdot \pi)(2^\alpha v_{X_\alpha}) = \varepsilon_X(2^\alpha v_{\pi(X_\alpha)})$$

et de la classification des petits vecteurs donnée au théorème II.2.

#### 4. PREMIÈRES PROPRIÉTÉS DE $G = \text{Aut } U$ .

4.1. *Les transformations  $\gamma_T$ .* — Soit  $T \subset \Omega$  un plan vectoriel.

Désignons par  $\gamma_T$  la symétrie orthogonale par rapport à l'espace

$$\bigoplus_{i \in \Omega \bmod T} \mathbf{Q} \cdot v_{\tau_i(T)}.$$

En d'autres termes,  $\gamma_T$  est l'involution déterminée de la manière suivante :

Soit  $i \in \Omega$ . Si  $\tau_i(T)$  est le plan affine parallèle à  $T$  qui contient  $i$ , on a

$$\gamma_T(v_i) = \frac{1}{2} v_{\tau_i(T)} - v_i.$$

Soit  $\pi$  un élément de  $\text{Af}(\Omega)$ , et soit  $\vec{\pi}$  sa composante sur  $\text{GL}(\Omega)$ . Soient  $X$  un élément de  $\mathfrak{V}_{d-2}$ ,  $H$  un élément de  $\mathfrak{V}_{d-1}$ ,  $T$ ,  $T_1$  et  $T_2$  des éléments de  $\vec{\mathfrak{V}}_2$ .

Un calcul facile permet de vérifier les formules suivantes :

$$(1) \quad \pi \cdot \gamma_T \cdot \pi^{-1} = \gamma_{\vec{\pi}(T)}.$$

(2) Si  $V$  est une variété affine telle que  $T \subset \vec{V}$  :

$$\gamma_T \cdot \varepsilon_V \cdot \gamma_T = \varepsilon_V.$$

(3) Si  $T = \{0, t, t', t + t'\}$  et si  $T \cap \vec{X} = \{0, t'\}$  :

$$\gamma_T \cdot \varepsilon_X \cdot \gamma_T = \sigma(X + \tau_t(X); t') \cdot \varepsilon_{\tau_t(X)}.$$

(3') Si  $T = \{0, t, t', t + t'\}$  et si  $T \cap \vec{H} = \{0, t'\}$  :

$$\eta_T \cdot \varepsilon_H \cdot \eta_T = \tau_{t'} \cdot \varepsilon_{\Omega + X}.$$

(4) Si  $T \cap \vec{X} = \{0\}$  :

$$\eta_T \cdot \varepsilon_X \cdot \eta_T = \varepsilon_{\Omega + X} \cdot \eta_T \cdot \varepsilon_X.$$

Soit

$$\eta_T \cdot \varepsilon_X \cdot \eta_T = - \varepsilon_X \cdot \eta_T \cdot \varepsilon_X.$$

(5) Si  $T_1 \cap T_2$  est une droite,  $T_1 \cap T_2 = \{0, u\}$  :

$$\eta_{T_1} \cdot \eta_{T_2} = \eta_{\overrightarrow{(T_1 + T_2)}} \cdot \tau_u.$$

(6) Si  $T_1 \cap T_2 = \{0\}$  :

$$(\eta_{T_1} \cdot \eta_{T_2})(v_0) = \frac{1}{4} \varepsilon_{T_1 + T_2}(v_{T_1 + T_2}),$$

d'où

$$(\eta_{T_1} \cdot \eta_{T_2})(v_i) = \frac{1}{4} \varepsilon_{\tau_i(T_1 + T_2)}(v_{\tau_i(T_1 + T_2)}).$$

Si  $S$  est une variété affine de dimension  $a$ , désignons par  $S_T$  la variété affine d'espace vectoriel associé  $\vec{S} + T$  qui contient  $S$  :  $S_T$  est une variété de dimension  $a$ ,  $a + 1$  ou  $a + 2$  selon que  $T \subset \vec{S}$ ,  $|T \cap \vec{S}| = 2$  ou  $|T \cap \vec{S}| = 1$ . Il est alors immédiat de vérifier les formules :

(7) Si  $T \subset \vec{S}$  :  $\eta_T(v_s) = v_s$ .

(8) Si  $T \cap \vec{S}$  est une droite :  $\eta_T(v_s) = v_{(s_T + s)}$ .

(9) Si  $T \cap \vec{S} = \{0\}$  :  $\eta_T(v_s) = \frac{1}{2} \varepsilon_s(v_{s_T})$ .

THÉORÈME II.4 :

(1) Pour tout plan vectoriel  $T$ ,  $\eta_T$  est un automorphisme du réseau  $U$ .

(2) Le groupe  $G = \text{Aut } U$  est transitif sur les petits vecteurs de  $U$ .

Démonstration du théorème II.4. — Soit  $T = \{0, t, t', t + t'\} \in \vec{\mathcal{V}}_2$ , et soit  $X_\alpha \in \mathcal{V}_{2m-2\alpha}$ .

Si  $T \cap \vec{X}_\alpha = \{0, t\}$ , posons  $Y_\alpha = \tau_t(X_\alpha)$ .

Si  $T \cap \vec{X}_\alpha = \{0\}$ , posons  $X_{\alpha-1} = (X_\alpha)_T$  : on a  $X_{\alpha-1} \in \mathcal{V}_{2m-2(\alpha-1)}$ . Il résulte des formules (7), (8) et (9) :

(7') Si  $T \subset \vec{X}_\alpha$ ,  $\eta_T(2^\alpha v_{X_\alpha}) = 2^\alpha v_{X_\alpha}$ .

(8') Si  $T \cap \vec{X}_\alpha = \{0, t\}$ ,  $\eta_T(2^\alpha v_{X_\alpha}) = 2^\alpha v_{Y_\alpha}$ .

(9') Si  $T \cap \vec{X}_\alpha = \{0\}$ ,  $\eta_T(2^\alpha v_{X_\alpha}) = \varepsilon_{X_\alpha}(2^{\alpha-1} \cdot v_{X_{\alpha-1}})$ .

Des formules (7'), (8') et (9'), on déduit alors :

1° Les images par  $\gamma_T$  des générateurs de  $U$  appartiennent à  $U$ . Donc  $\gamma_T(U) \subset U$ , et par suite  $\gamma_T \in G = \text{Aut } U$ .

2° De la formule (9'), on déduit que pour tout  $\alpha$  ( $0 < \alpha \leq m$ ), il existe un vecteur de  $P_\alpha$  et  $T \in \vec{\mathfrak{V}}_2$  tels que l'image par  $\gamma_T$  de ce vecteur soit dans  $P_{\alpha-1}$ . De 1° et de la transitivité de  $N$  sur chaque  $P_\alpha$  ( $0 \leq \alpha \leq m$ ), il résulte bien la transitivité de  $G$  sur  $\bigcup_{\alpha=0}^m P_\alpha$ .

4.2. *Partition stable sur l'ensemble des petits vecteurs de  $U$ . Ordre de  $G$ .*

**THÉORÈME II.5.** — *Les transformés distincts par  $G$  de l'ensemble  $P_m = \{ \pm 2^m v_i \mid i \in \Omega \}$  forment une partition de l'ensemble des petits vecteurs de  $U$ .*

*Démonstration du théorème II.5.* — Il nous suffit de démontrer que si  $\sigma$  est un automorphisme de  $U$  tel que  $\sigma(P_m) \cap P_m \neq \emptyset$ , alors  $\sigma(P_m) = P_m$ , c'est-à-dire  $\sigma \in N$ . Pour cela, puisque  $N$  est transitif sur  $P_m$ , nous pouvons supposer que  $\sigma(v_0) = v_0$ .

Comme  $\sigma$  laisse fixe  $2^m v_0$ ,  $\sigma$  opère sur l'ensemble des petits vecteurs de  $U^0$  qui ont un produit scalaire avec  $2^m v_0$  égal à 2 ou à  $-2$ . Or cet ensemble est manifestement l'ensemble que nous avons désigné par  $\vec{P}'_1$  au paragraphe 2. Il résulte du corollaire 2 du théorème II.2 que  $\sigma$  fixe globalement  $U^0 \cap 2R$ , engendré par  $\vec{P}'_1$ . Donc  $\sigma$  fixe  $\frac{1}{2}U^0 \cap R$ , et fixe également le réseau dual  $2U + 2^m R$ .

Si  $\sigma(P_m) \neq P_m$ , il existe un entier  $\alpha$  strictement inférieur à  $m$  et un élément  $x$  de  $P_m$  tel que  $\sigma(x) \in P_\alpha$ . Mais puisque  $\sigma$  conserve  $2U + 2^m R$ , et  $x \in 2^m R$ , on a  $\sigma(x) \in 2U + 2^m R$ . Ainsi  $(2U + 2^m R) \cap P_\alpha \neq \emptyset$ . Selon le théorème II.3 (2),  $P_\alpha$  est une orbite selon  $N$  opérant dans l'ensemble des petits vecteurs de  $U$ . Par définition  $N$  laisse globalement fixe  $2U + 2^m R$ . Donc

$$P_\alpha \subset 2U + 2^m R.$$

Selon le corollaire 2 du théorème II.2,  $P_\alpha$  engendre  $U \cap 2^\alpha R$ . On a donc

$$U \cap 2^\alpha R \subset 2U + 2^m R.$$

Utilisant les notations du chapitre I (§ 1), on peut donc écrire

$$\varphi_U(U \cap 2^\alpha R) \subset \varphi_U(2^m R) \quad \text{soit} \quad \bar{R}^\alpha(U) \subset \bar{R}^m(U).$$

Le théorème I.2 permet de calculer les dimensions de ces espaces :  
 $\dim \bar{R}^\alpha(U) = \dim \bar{U}_{m-\alpha}^0(R) = \dim \bar{U}_{\alpha-1}(R^0) = n - \dim \bar{U}_{\alpha-1}(R) = n - \dim \langle \mathfrak{V}_{2m-2\alpha+2} \rangle$ ,  
 $\dim \bar{R}^m(U) = \dim \bar{U}_0^0(R) = \dim \bar{U}_{m-1}(R^0) = n - \dim \bar{U}_{m-1}(R) = n - \dim \langle \mathfrak{V}_2 \rangle$ .

Si  $\alpha < m$ , on a  $\dim \bar{R}^\alpha(U) > \dim R(U)$ , et l'hypothèse  $\sigma(P_m) \neq P_m$  est absurde, ce qui démontre le théorème II.5.

Nous désignerons par  $\mathcal{R}$  la partition de l'ensemble des petits vecteurs de  $U$  définie par les transformés distincts de  $P_m$  par le groupe  $G = \text{Aut } U$ .

Comme le stabilisateur de  $P_m$  dans  $G$  est le groupe  $N$ , la « partition stable »  $\mathcal{R}$  est isomorphe, comme  $G$ -ensemble, à l'espace homogène  $G/N$ .

COROLLAIRE :

(1) L'ordre du groupe  $G = \text{Aut } U$  est

$$|G| = |GL_d(\mathbf{F}_2)| \cdot 2^{1+2d+\binom{d}{2}} \left( \sum_{\alpha=0}^m 2^{\binom{2m-2\alpha}{2}} \nu(2m-2\alpha, d) \right).$$

(2) Si  $T \in \vec{\mathfrak{V}}_2$ , le groupe  $G$  est engendré par  $N$  et par  $\eta_T$ .

Démonstration du corollaire :

1° On a évidemment  $|G| = |\mathcal{R}| \cdot |N|$ .

D'une part,  $|N| = |\langle \mathfrak{V}_{d-2} \rangle| \cdot |\text{Af}(\Omega)|$  d'après le théorème II.3. Comme  $\langle \mathfrak{V}_{d-2} \rangle$  est de dimension  $1 + d + \binom{d}{2}$  sur  $\mathbf{F}_2$  on trouve

$$|N| = 2^{1+2d+\binom{d}{2}} |GL_d(\mathbf{F}_2)|.$$

D'autre part, si  $\delta$  est le nombre de petits vecteurs de  $U$ , on a  $|\mathcal{R}| = \frac{\delta}{|P_m|}$ . Comme  $|P_m| = 2^{d+1}$ , il nous suffit d'appliquer la formule donnant  $\delta$  (corollaire 1 au théorème II.2) pour trouver la formule écrite dans l'énoncé du corollaire.

2° Il résulte de 4.1, formule (1), que si  $T \in \vec{\mathfrak{V}}_2$ , le groupe engendré par  $N$  et  $\eta_T$  contient toutes les transformations  $\eta_{T'}$ , pour  $T' \in \vec{\mathfrak{V}}_2$ . De la démonstration du théorème II.4, on déduit alors que ce groupe est transitif sur l'ensemble des petits vecteurs de  $U$ , donc sur  $\mathcal{R}$ . Comme ce groupe contient  $N$ , stabilisateur de  $P_m$ , il est égal à  $G$ .

5. OPÉRATION DE  $G$  SUR  $\mathcal{R} \simeq G/N$ . — Nous allons déterminer le noyau de l'opération de  $G$  dans  $G/N$ , et montrer que cette opération est primitive.

Nous désignons par  $F$  le groupe  $E (\langle \mathcal{V}_{d-1} \rangle)$ , et par  $A$  le groupe  $\mathfrak{E}(\Omega) \rtimes F$ .

**THÉORÈME II.6.** — *Le noyau de l'opération de  $G$  dans  $G/N$  est*

$$\bigcap_{s \in G} s \cdot N \cdot s^{-1} = A.$$

*Démonstration du théorème II.6 :*

1° *Le groupe  $A$  est distingué dans  $G$ .*

D'après le corollaire du théorème II.5 (2) il suffit de démontrer que les conjugués par  $N$  et par une transformation  $\gamma_T$  de tout élément de  $A$  sont encore dans  $A$ .

Soit donc  $T \in \vec{\mathcal{V}}_2$  et  $\tau_t \cdot \varepsilon_H \in A$ .

Soit  $\pi \in \text{Af}(\Omega)$ , et soit  $\vec{\pi}$  sa composante sur  $GL(\Omega)$ . Il est clair que

$$\pi \cdot (\tau_t \cdot \varepsilon_H) \cdot \pi^{-1} = \tau_{\vec{\pi}(t)} \cdot \varepsilon_{\pi(H)} \in A.$$

Soit  $X \in \langle \mathcal{V}_{d-2} \rangle$ . On a

$$\varepsilon_X \cdot (\tau_t \cdot \varepsilon_H) \cdot \varepsilon_X^{-1} = \tau_t \cdot \varepsilon_{H \dot{+} (X \dot{+} \tau_t(X))}.$$

D'après le corollaire 1 de la proposition I.4, on a  $X \dot{+} \tau_t(X) \in \langle \mathcal{V}_{d-1} \rangle$ , et par conséquent  $\varepsilon_X \cdot (\tau_t \cdot \varepsilon_H) \cdot \varepsilon_X^{-1} \in A$ .

Enfin, pour la conjugaison par  $\gamma_T$ , distinguons deux cas :

Si  $T \subset \vec{H}$  ou si  $H = \emptyset$ ,  $\gamma_T$  centralise  $\tau_t \cdot \varepsilon_H$  [4.1, formules (1) et (2)];

Si  $T \cap \vec{H} = \{0, u\}$ ,  $\gamma_T \cdot (\tau_t \cdot \varepsilon_H) \cdot \gamma_T = \tau_{t+u} \cdot \varepsilon_{\Omega \dot{+} H}$  [4.1, formule (3')], donc  $\gamma_T \cdot (\tau_t \cdot \varepsilon_H) \cdot \gamma_T \in A$ .

2° *Les sous-groupes distingués de  $N$  contenant  $A$ .*

Soit  $K$  un sous-groupe propre distingué de  $N$  contenant  $A$ . Nous allons démontrer que  $K \subset \mathfrak{E}(\Omega) \rtimes E$ .

On a

$$K \cdot E / E \subset N / E \simeq \text{Af}(\Omega).$$

Or les sous-groupes distingués de  $\text{Af}(\Omega)$  sont  $\{1\}$ ,  $\mathfrak{E}(\Omega)$  ou  $\text{Af}(\Omega)$ .

Par conséquent, soit  $K \subset E$ , soit  $K \cdot E = \mathfrak{E}(\Omega) \cdot E$ , soit  $K \cdot E = N$ . Comme  $K \supset A$ , on ne peut avoir  $K \subset E$ . Pour démontrer que  $K \subset \mathfrak{E}(\Omega) \cdot E$  il nous suffit donc de démontrer que si  $K \cdot E = N$ , alors  $K \supset E$ . Soit  $E_1 = K \cap E$ . On a

$$[\text{Af}(\Omega), E] \subset [N, E] = [K \cdot E, E] \subset [K, E] \subset E_1.$$

Or (corollaire 2 de la proposition I.4) on sait que  $[Af(\Omega), E] = E$ . D'où  $E \subset E_1$ , et par suite  $E = E_1$  et  $K \supset E$ .

3° *Démontrons que*  $\bigcap_{s \in G} s.N.s^{-1} = A$ .

Posons, provisoirement,

$$\dot{N} = \bigcap_{s \in G} s.N.s^{-1}.$$

D'après ce qui précède, on a donc

$$A \subset \dot{N} \subset \mathfrak{F}(\Omega).E.$$

De plus,  $\dot{N}$  est l'ensemble des éléments de  $G$  qui opèrent trivialement modulo  $N$ , c'est-à-dire qui fixent globalement chaque transformé de  $P_m$ . En particulier, tout élément de  $\dot{N}$  transforme un petit vecteur en lui-même, en son opposé, ou en un vecteur orthogonal.

Pour démontrer que  $\dot{N} = A$ , il nous suffit donc de montrer que pour tout élément de  $\mathfrak{F}(\Omega).E$  qui n'est pas dans  $A$ , il existe un petit vecteur qui n'est transformé par cet élément ni en lui-même, ni en son opposé, ni en un vecteur orthogonal. En fait, comme par définition  $A = \mathfrak{F}(\Omega).F$ , il est clair qu'il nous suffit de démontrer que pour tout élément de  $E$  qui n'est pas dans  $F$ , il existe un petit vecteur qui n'est transformé par cet élément ni en lui-même, ni en son opposé, ni en un vecteur orthogonal.

Soit donc  $\varepsilon_x \in E$ ,  $X \notin \langle \mathcal{V}_{d-1} \rangle$ . Comme  $\langle \mathcal{V}_{d-1} \rangle = \langle \mathcal{V}_2 \rangle^0$ , il existe  $T \in \mathcal{V}_2$  tel que  $|X \cap T| \equiv 1 \pmod{2}$ . Alors  $\varepsilon_x(2^{m-1}v_T)$  est différent de  $\pm 2^{m-1}v_T$  et

$$\varepsilon_x(2^{m-1}v_T).2^{m-1}v_T = (2^{m-1}v_T - 2^m v_{X \cap T}).2^{m-1}v_T = 2^m - 2^{m-1}|X \cap T| \neq 0.$$

**COROLLAIRE.** — *La partition  $\mathcal{R}$  est plus fine que la partition définie par les orbites de  $N$  dans l'ensemble des petits vecteurs de  $U$ . Plus précisément :*

*Soit  $\varepsilon_x(2^\alpha v_{x_\alpha}) \in P_\alpha$  ( $0 \leq \alpha \leq m$ ,  $X_\alpha \in \mathcal{V}_{2m-2\alpha}$  et  $X \in \langle \mathcal{V}_{d-2} \rangle$ ). L'élément de la partition  $\mathcal{R}$  qui contient  $\varepsilon_x(2^\alpha v_{x_\alpha})$  est*

$$\mathcal{R}(\varepsilon_x(2^\alpha v_{x_\alpha})) = \left\{ \varepsilon_{H \dot{+} X}(2^\alpha v_{y_\alpha}) \mid (\vec{Y}_\alpha = \vec{X}_\alpha) \text{ et } (H \in \langle \mathcal{V}_{d-1} \rangle) \right\}.$$

*Démonstration du corollaire.* — Il est facile de vérifier que le groupe  $A$  est transitif sur l'ensemble  $P_m$ . Or  $A$  est distingué dans  $G$  : il opère donc transitivement sur chaque transformé de  $P_m$ . Par conséquent, le transformé de  $P_m$  qui contient un petit vecteur est égal à l'ensemble des transformés de ce vecteur par le groupe  $A$ ; le corollaire s'en déduit immédiatement.

THÉORÈME II.7. — *Le groupe G opère primitivement dans  $\mathcal{R} \simeq G/N$ .*

*Démonstration.* — Nous voulons démontrer qu'il n'y a pas de partition de l'ensemble  $\mathcal{R}$ , non triviale, non grossière, et stable par G. Considérons donc une partition de  $\mathcal{R}$ ,  $\mathcal{R} = \mathcal{R}_0 \cup \mathcal{R}_1 \cup \dots \cup \mathcal{R}_l$ , stable par G et non triviale : chaque élément de la partition est au moins de cardinal 2. Supposons que  $P_m$  appartienne à  $\mathcal{R}_0$ . Il faut démontrer que cette partition est la partition grossière, c'est-à-dire que  $l = 0$  et  $\mathcal{R}_0 = \mathcal{R}$ .

1° Nous savons que si  $P \in \mathcal{R}$ , il existe  $\alpha$  ( $0 \leq \alpha \leq m$ ) tel que  $P \subset P_\alpha$  (corollaire du théorème II.6). D'autre part, les orbites de N dans l'ensemble des petits vecteurs sont les  $P_\alpha$  ( $0 \leq \alpha \leq m$ ) (théorème II.3). Par conséquent, les orbites de N dans  $\mathcal{R}$  sont les ensembles

$$\mathcal{N}_\alpha = \{ P \mid (P \in \mathcal{R}) \text{ et } (P \subset P_\alpha) \} \quad (0 \leq \alpha \leq m).$$

La classe  $\mathcal{R}_0$  contient  $P_m$ ; elle est réunion d'orbites de N dans  $\mathcal{R}$ , puisque N est le stabilisateur de  $P_m$ . D'après notre hypothèse,  $\mathcal{R}_0$  est réunion d'au moins deux orbites de N : il existe  $\alpha$  ( $0 \leq \alpha < m$ ) tel que  $\mathcal{N}_\alpha \subset \mathcal{R}_0$ .

2° Le théorème II.7 est donc démontré dès que l'assertion suivante est démontrée :

*Si  $0 < \beta < m$ , pour que  $\mathcal{R}_0$  contienne  $\mathcal{N}_\beta$ , il faut et il suffit que  $\mathcal{R}_0$  contienne  $\mathcal{N}_{\beta-1}$ .*

(a) *Supposons que  $\mathcal{R}_0$  contienne  $\mathcal{N}_\beta$ .*

Soit  $T \in \vec{\mathcal{V}}_2$ .

Puisque  $\beta < m$ , il existe  $X_\beta \in \mathcal{V}_{2m-2\beta}$  tel que  $T \subset \vec{X}_\beta$ . La transformation  $\gamma_{IT}$  fixe le vecteur  $2^\beta v_{X_\beta} \in P_\beta$ , donc  $\gamma_{IT}$  fixe l'élément de la partition  $\mathcal{R}$  qui contient  $2^\beta v_{X_\beta}$ ; d'après l'hypothèse, cet élément est  $\mathcal{R}_0$ , donc  $\gamma_{IT}$  fixe  $\mathcal{R}_0$ .

Puisque  $\beta > 0$ , il existe  $Y_\beta \in \mathcal{V}_{2m-2\beta}$  tel que  $T \cap \vec{Y}_\beta = \{0\}$ . On sait qu'alors  $\gamma_{IT}(2^\beta v_{Y_\beta}) \in P_{\beta-1}$  [4.1, formule (9)]. Comme  $\gamma_{IT}$  fixe  $\mathcal{R}_0$ , on en déduit que  $\mathcal{R}_0 \cap \mathcal{N}_{\beta-1} \neq \emptyset$ . Donc  $\mathcal{N}_{\beta-1} \subset \mathcal{R}_0$ .

(b) *Supposons que  $\mathcal{R}_0$  contienne  $\mathcal{N}_{\beta-1}$ .*

Soit  $T \in \vec{\mathcal{V}}_2$ . La transformation  $\gamma_{IT}$  fixe tout vecteur du type  $2^{\beta-1} v_{X_{\beta-1}}$  où  $T \subset \vec{X}_{\beta-1}$ . Elle fixe donc  $\mathcal{R}_0$ . Choisissons  $X'_\beta \in \mathcal{V}_{2m-2\beta}$  tel que  $\vec{X}'_\beta \cap T = \{0\}$ . On sait que  $\gamma_{IT}(2^\beta v_{X'_\beta}) \in P_{\beta-1}$ . Posons  $x_{\beta-1} = \gamma_{IT}(2^\beta v_{X'_\beta})$ . On a alors  $\gamma_{IT}(x_{\beta-1}) = 2^\beta v_{X'_\beta}$ , donc  $\gamma_{IT}(x_{\beta-1}) \in P_\beta$  : par un raisonnement analogue à celui fait en (a), on en déduit que  $\mathcal{R}_0$  contient  $\mathcal{N}_\beta$ .

C. Q. F. D.

6. SIMPLICITÉ DU GROUPE  $G/A$ . — Pour démontrer la simplicité du groupe  $G/A$ , nous utilisons le théorème suivant :

THÉORÈME. — Soit  $G$  un groupe, et soit  $N$  un sous-groupe maximal de  $G$ . Supposons que :

- (1)  $G$  est égal à son groupe de commutateurs.
- (2)  $N$  contient un sous-groupe abélien  $E$  distingué dans  $N$  et la réunion des conjugués de  $E$  engendre  $G$ .

Alors le quotient de  $G$  par l'intersection des conjugués de  $N$  est un groupe simple.

(On en trouvera la démonstration, d'ailleurs fort simple dans DIEUDONNÉ, *La Géométrie des groupes classiques*, 2<sup>e</sup> édition, p. 39.)

Nous allons vérifier que les groupes  $N$  et  $E$  précédemment définis dans  $G$  satisfont bien aux hypothèses du théorème.

1°  $N$  est maximal dans  $G$  [En effet,  $G$  opère primitivement dans  $G/N$  (théorème II.7)] et  $E$  est distingué dans  $N$  et abélien.

2° La réunion des conjugués de  $E$  engendre  $G$ .

Désignons, provisoirement, par  $\bar{E}$  le groupe engendré par la réunion de conjugués de  $E$  dans  $G$ .

On a évidemment :  $\bar{E} \triangleleft G$ .

a. Soit  $T = \{0, t, t', t + t'\} \in \vec{\mathcal{V}}_2$  et soit  $X \in \vec{\mathcal{V}}_{d-2}$  tel que  $X \cap T = \{0, t'\}$ . On sait alors que [4.1, formule (3)] :

$$\gamma_T \cdot \varepsilon_X \cdot \gamma_T \cdot \varepsilon_{\tau_t(X)} = \sigma(X \dot{+} \tau_t(X); t') \in GL(\Omega).$$

On en déduit que  $\bar{E} \cap GL(\Omega) \neq \{1\}$ , et comme  $GL(\Omega)$  est simple, on a  $\bar{E} \supset GL(\Omega)$ .

b. D'après le paragraphe 5, démonstration du théorème 5.2, un sous-groupe distingué  $K$  de  $N$  vérifie toujours l'une des trois propriétés suivantes :  $K \subset E$ , ou  $K.E = \mathfrak{S}(\Omega).E$ , ou  $K.E = N$ .

En appliquant ce résultat à  $K = \bar{E} \cap N$ , et en utilisant les propriétés  $GL(\Omega) \subset \bar{E}$  et  $E \subset \bar{E}$  on trouve que  $\bar{E} \supset N$ .

Comme  $N$  est maximal non distingué, on en déduit que  $\bar{E} = G$ .

On a d'ailleurs [4.1, formule (4)] :

$$(-\varepsilon_X) \cdot (\gamma_T \cdot \varepsilon_X \cdot \gamma_T) \cdot \varepsilon_X = \gamma_T,$$

ce qui nous permet de vérifier que  $\gamma_T \in \bar{E}$ .

3°  $G$  est égal à son groupe des commutateurs.

D'après 2°, il nous suffit évidemment de démontrer que  $E$  est contenu dans le groupe dérivé  $[G, G]$ .

Or on sait (corollaire 2 de la proposition I.4) que :  $[E, \text{Af}(\Omega)] = E$ , ce qui prouve évidemment que  $E \subset [G, G]$ .

**THÉORÈME II.8.** — *Le groupe  $G/A$  est un groupe simple, d'ordre*

$$|G/A| = |GL_d(\mathbf{F}_2)| \cdot 2^{\binom{d}{2}} \left( \sum_{\alpha=0}^m 2^{\binom{2m-2\alpha}{2}} \nu(2m-2\alpha, d) \right).$$

## 7. IDENTIFICATION DU GROUPE $G/A$ .

**THÉORÈME II.9.** — *Le groupe  $G/A$  est isomorphe au groupe de Chevalley de type  $D_d$  sur le corps à deux éléments.*

*Démonstration du théorème II.9.* — Si  $s \in G$  (resp.  $K \subset G$ ), nous désignons par  $\bar{s}$  (resp.  $\bar{K}$ ) son image dans  $G/\{-\text{Id}, +\text{Id}\}$ . Il est clair que  $G/A$  est isomorphe à  $\bar{G}/\bar{A}$ . Nous allons démontrer que  $\bar{G}/\bar{A}$  se représente comme le groupe dérivé du groupe orthogonal d'une forme quadratique non dégénérée d'indice  $d$  sur un  $\mathbf{F}_2$ -espace vectoriel de dimension  $2d$ .

1° *Espace  $\bar{A}$*  : Par définition,  $A = \mathfrak{G}(\Omega) \rtimes F$ . Si  $t \in \Omega$  et si  $H \in \langle \mathfrak{V}_{d-1} \rangle$ , on sait que

$$\tau_t \cdot \varepsilon_H = \varepsilon_{\tau_t(H)} \cdot \tau_t.$$

Comme  $\langle \mathfrak{V}_{d-1} \rangle = \mathfrak{V}_{d-1} \cup \{\emptyset, \Omega\}$  il est clair que ou bien  $\tau_t(H) = H$ , ou bien  $\tau_t(H) = H \dot{+} \Omega$ , et par conséquent :  $\varepsilon_{\tau_t(H)}$  et  $\varepsilon_H$  ont même image modulo  $\{\varepsilon_\Omega, \varepsilon_\emptyset\} = \{-\text{Id}, +\text{Id}\}$ . On a donc

$$\bar{\tau}_t \cdot \bar{\varepsilon}_H = \bar{\varepsilon}_H \cdot \bar{\tau}_t \quad \text{et} \quad \bar{A} = \bar{\mathfrak{G}}(\Omega) \times \bar{F};$$

$\bar{A}$  est donc un groupe abélien 2-élémentaire isomorphe à  $\mathbf{F}_2^{2d}$ .

Comme  $\bar{A}$  est distingué et abélien,  $\bar{G}/\bar{A}$  opère évidemment sur  $\bar{A}$ . Nous allons munir  $\bar{A}$  d'une forme quadratique  $Q$  pour laquelle l'opération de  $\bar{G}/\bar{A}$  est orthogonale.

2° *Forme quadratique sur  $\bar{A}$*  :

(a)  $\bar{F} = \overline{E(\langle \mathfrak{V}_{d-1} \rangle)}$  s'identifie au dual du  $\mathbf{F}_2$ -espace vectoriel  $\bar{\mathfrak{G}}(\Omega) \simeq (\mathbf{F}_2)^d$  : à  $\bar{\varepsilon}_H \in \bar{F}$ ,  $\bar{\varepsilon}_H \neq \bar{1}$ , nous associons la forme linéaire sur  $\bar{\mathfrak{G}}(\Omega)$ ,  $\mu_H$ , qui s'annule sur  $\vec{H}$ ; il est facile de voir qu'à  $\bar{\varepsilon}_H \cdot \bar{\varepsilon}_{H'} = \bar{\varepsilon}_{H \dot{+} H'}$  correspond  $\mu_H + \mu_{H'}$ .

(b) L'espace  $\bar{A} = \mathfrak{G}(\bar{\Omega}) \times \bar{F}$  est donc muni d'une forme symplectique canonique  $f$  définie ainsi :

$$\begin{aligned} \bar{\mathfrak{G}}(\Omega) \text{ et } \bar{F} \text{ sont totalement isotropes,} \\ f(\bar{\tau}_t, \bar{\varepsilon}_H) = 0 \quad \text{si } t \in \vec{H} \text{ ou } H = \emptyset, \\ f(\bar{\tau}_t, \bar{\varepsilon}_H) = 1 \quad \text{si } t \notin \vec{H}. \end{aligned}$$

Il existe alors une et une seule forme quadratique  $Q$ , pour laquelle  $\bar{\mathfrak{G}}(\Omega)$  et  $\bar{F}$  sont totalement singuliers et de forme bilinéaire associée  $f$ .

On a

$$Q(\bar{\tau}_t, \bar{\varepsilon}_H) = f(\bar{\tau}_t, \bar{\varepsilon}_H).$$

3°  $\bar{G}/\bar{A}$  opère orthogonalement dans  $\bar{A}$  :

Soit  $\tau_t, \varepsilon_H \in A$ . Nous allons vérifier que, pour tout  $s \in G$ ,

$$Q(\bar{s}, \bar{\tau}_t, \bar{\varepsilon}_H, \bar{s}^{-1}) = Q(\bar{\tau}_t, \bar{\varepsilon}_H).$$

Comme  $G$  est engendré par  $N$  et un  $\gamma_T$  ( $T \in \vec{\mathfrak{V}}_2$ ), il suffit de le vérifier pour les éléments de  $N$  et pour un  $\gamma_T$  bien choisi.

(a) Soit  $\pi \in \text{Af}(\Omega)$ . On a

$$\pi \cdot \tau_t \cdot \varepsilon_H \cdot \pi^{-1} = \tau_{\pi(t)} \cdot \varepsilon_{\pi(H)},$$

donc

$$Q(\bar{\pi}, \bar{\tau}_t, \bar{\varepsilon}_H, \bar{\pi}^{-1}) = f(\bar{\tau}_{\pi(t)}, \bar{\varepsilon}_{\pi(H)}),$$

quantité manifestement égale d'après la définition de  $f$ , à  $f(\bar{\tau}_t, \bar{\varepsilon}_H) = Q(\tau_t, \varepsilon_H)$ .

(b) Soit  $X \in \mathfrak{V}_{d-2}$ . On a

$$\varepsilon_X \cdot \tau_t \cdot \varepsilon_H \cdot \varepsilon_X^{-1} = \tau_t \cdot \varepsilon_H \cdot \varepsilon_{X + \tau_t(X)},$$

d'où

$$Q(\bar{\varepsilon}_X, \bar{\tau}_t, \bar{\varepsilon}_H, \bar{\varepsilon}_X^{-1}) = f(\bar{\tau}_t, \bar{\varepsilon}_H, \bar{\varepsilon}_{X + \tau_t(X)}) = f(\bar{\tau}_t, \bar{\varepsilon}_H) + f(\bar{\tau}_t, \bar{\varepsilon}_{X + \tau_t(X)}).$$

Comme  $X + \tau_t(X)$  est soit vide, soit un hyperplan dont la direction vectorielle contient  $t$ , on a

$$f(\bar{\tau}_t, \bar{\varepsilon}_{X + \tau_t(X)}) = 0, \quad \text{donc } Q(\bar{\varepsilon}_X, \bar{\tau}_t, \bar{\varepsilon}_H, \bar{\varepsilon}_X^{-1}) = Q(\bar{\tau}_t, \bar{\varepsilon}_H).$$

c. Choisissons  $T \in \vec{\mathfrak{V}}_2$  tel que  $\gamma_T$  commute avec  $\varepsilon_H$  : Si  $H \neq \emptyset$ , il suffit de choisir  $T \subset \vec{H}$ . On sait qu'alors  $\gamma_T$  centralise  $\tau_t, \varepsilon_H$  et par conséquent :

$$Q(\bar{\gamma}_T, \bar{\tau}_t, \bar{\varepsilon}_H, \bar{\gamma}_T^{-1}) = Q(\bar{\tau}_t, \bar{\varepsilon}_H).$$

Ainsi le groupe  $\overline{G}/\overline{A}$  se plonge dans le groupe orthogonal de la forme  $Q$ , noté  $O(Q)$ . Comme  $\overline{G}/\overline{A}$  est simple non abélien, donc égal à son groupe dérivé,  $\overline{G}/\overline{A}$  se plonge en fait dans le groupe dérivé de  $O(Q)$ ; ce groupe dérivé est d'indice 2 dans  $O(Q)$  et égal au groupe  $O^+(Q)$  (voir DIEUDONNÉ, *La Géométrie des groupes classiques*, § 10). Nous allons démontrer que  $\overline{G}/\overline{A} \simeq O^+(Q)$ , ce qui achèvera la démonstration du théorème, puisque  $O^+(Q)$  est le groupe simple de Chevalley de type  $D_d$  sur  $F_2$ .

4° *Identification de  $\overline{G}/\overline{A}$  avec  $O^+(Q)$*  : Considérons l'opération du groupe  $O(Q)$  sur l'ensemble des sous-espaces totalement singuliers maximaux de  $\overline{A}$ . On sait que :

(1) L'orbite de  $O^+(Q)$  qui contient  $\overline{F}$  est formée de l'ensemble  $\mathcal{F}$  des sous-espaces totalement singuliers maximaux de  $\overline{A}$  dont l'intersection avec  $\overline{F}$  a une dimension de même parité que la dimension de  $\overline{F}$ . Avec les notations de l'appendice, l'orbite de  $O^+(Q)$  sur  $\overline{F}$  est donc :

$$\bigcup_{\alpha=0}^{\alpha=m} S_{d-2\alpha}(\overline{F}).$$

(2) Le stabilisateur de  $\overline{F}$  dans  $O(Q)$ , noté  $O_{\overline{F}}$ , est produit semi-direct d'un groupe isomorphe à  $GL_d(F_2)$  par un groupe distingué 2-abélien élémentaire d'ordre  $2^{\frac{d(d-1)}{2}}$  (d'après l'Appendice). De plus, les orbites de ce groupe  $O_{\overline{F}}$  dans l'ensemble des sous-espaces totalement singuliers maximaux sont les ensembles  $S_a(\overline{F})$  ( $0 \leq a \leq d$ ).

Identifions maintenant  $\overline{G}/\overline{A}$  et  $O^+(Q)$ . Par abus de notation, considérons que  $\overline{G}/\overline{A} \subset O^+(Q)$ .

(a) Le stabilisateur de  $\overline{F}$  dans  $\overline{G}/\overline{A}$  est le groupe  $\overline{N}/\overline{A}$ . En effet, il est clair que  $F$  est distingué dans  $N$ . Comme  $N$  est maximal,  $N$  est le normalisateur de  $F$ .

(b) Or  $\overline{N}/\overline{A} = \overline{GL}(\Omega) \ltimes \overline{E}/\overline{F}$  est justement produit semi-direct d'un groupe isomorphe à  $GL_d(F_2)$  par un groupe abélien 2-élémentaire d'ordre  $2^{\frac{d(d-1)}{2}}$ . On en déduit donc que : si  $O_{\overline{F}}^+ = O^+(Q) \cap O_{\overline{F}}$ ,  $\overline{N}/\overline{A} = O_{\overline{F}}^+ = O_{\overline{F}}$ .

Pour démontrer que  $\overline{G}/\overline{A} = O^+(Q)$ , il nous suffit donc de démontrer que l'ensemble des transformés de  $\overline{F}$  par  $\overline{G}/\overline{A}$  est égal à  $\mathcal{F}$ .

(c) *Étudions donc l'ensemble des transformés de  $\overline{F}$  par le groupe de  $\overline{G}/\overline{A}$ .*

Puisque  $N$  est le normalisateur de  $F$ , l'opération de  $G$  sur l'ensemble des conjugués de  $F$  est équivalente à l'opération de  $G$  sur l'espace homogène  $G/N$ , laquelle est équivalente à l'opération de  $G$  sur  $\mathcal{R}$ , ou encore sur l'ensemble des transformés par  $G$  de l'ensemble  $P_m$ . A chaque transformé de  $P_m$  (c'est-à-dire du réseau  $R$ ) par  $G$  correspond donc un transformé de  $\bar{F}$  (et *vice versa*), de la manière suivante : si  $R' = s(R)$  est un transformé de  $R$  par  $s \in G$ ,  $s F s^{-1}$  est le groupe des changements de signes de la base  $\{s(v_i) \mid i \in \Omega\}$  portés par les éléments de  $\langle \mathfrak{V}_{d-1} \rangle$ .

Pour tout  $\alpha$  ( $0 \leq \alpha \leq m$ ), désignons par  $\mathcal{F}_\alpha$  l'ensemble des transformés de  $\bar{F}$  qui correspondent aux transformés de  $P_m$  contenus dans  $P_\alpha$ . On sait que les orbites de  $N$  sur  $\mathcal{R}$  sont les ensembles  $\{s(P_m) \mid (s \in G) \text{ et } s(P_m) \subset P_\alpha\}$  pour  $0 \leq \alpha \leq m$ .

Par conséquent les orbites de  $\bar{N}/\bar{A}$  sur l'ensemble des transformés de  $\bar{F}$  par  $\bar{G}/\bar{A}$  sont les ensembles  $\mathcal{F}_\alpha$  ( $0 \leq \alpha \leq m$ ). Donc l'orbite de  $\bar{F}$  par  $\bar{G}/\bar{A}$  est l'ensemble  $\bigcup_{\alpha=0}^{\alpha=m} \mathcal{F}_\alpha$ , dans lequel  $\bar{N}/\bar{A} = O_F^+$  a exactement  $(m+1)$  orbites. Comme  $\bar{G}/\bar{A}$  est contenu dans  $O^+(Q)$ , on a

$$\bigcup_{\alpha=0}^{\alpha=m} \mathcal{F}_\alpha \subset \mathcal{F}.$$

Or d'après (1) et (2),  $O_F^+$  a également  $(m+1)$  orbites dans  $\mathcal{F}$ . Par conséquent :

$$\bigcup_{\alpha=0}^{\alpha=m} \mathcal{F}_\alpha = \mathcal{F}.$$

Il en résulte immédiatement que  $\bar{G}/\bar{A} = O^+(Q)$ .

*Remarque.* — La démonstration précédente implique qu'il existe une permutation  $\varphi$  de l'ensemble des entiers du segment  $[0, m]$  telle que

$$\mathcal{F}_{\varphi(\alpha)} = S_{d-2\alpha}(\bar{F});$$

il s'agit de la permutation  $\alpha \rightarrow m - \alpha$ .

En effet, vérifions que si  $s(P_m) \subset P_\alpha$ , alors  $s\bar{F}s^{-1} \cap \bar{F}$  est de dimension  $d - 2(m - \alpha)$ . Pour cela il nous suffit de calculer  $s\bar{F}s^{-1}$  dans le cas où  $s(P_m) = \{\varepsilon_{II}(2^z v_{x_s}) \mid (H \in \langle \mathfrak{V}_{d-1} \rangle) \text{ et } (\vec{X}_\alpha = V_\alpha \text{ donnée dans } \vec{\mathfrak{V}}_{2m-2\alpha})\}$ . Or  $s\bar{F}s^{-1}$  est l'intersection avec  $A$  du sous-groupe de  $N$  qui transforme chaque vecteur de  $s(P_m)$  en lui-même ou en son opposé. Dans ce cas, il est facile de voir que

$$s F s^{-1} = \{\tau_t, \varepsilon_{II} \mid (t \in V_\alpha) \text{ et } (V_\alpha \subset \vec{H})\}.$$

On en déduit donc que

$$\bar{F} \cap s \bar{F} s^{-1} = \{ \bar{\varepsilon}_H \mid \vec{V}_\alpha \subset \vec{H} \},$$

et comme  $V_\alpha$  est de dimension  $2m - 2\alpha$ ,  $\bar{F} \cap s \bar{F} s^{-1}$  est bien de dimension  $d - (2m - 2\alpha)$ .

THÉORÈME II.10. — *Les suites exactes*

$$(S) \quad \{1\} \rightarrow A \rightarrow G \rightarrow G/A \rightarrow \{1\},$$

$$(\bar{S}) \quad \{1\} \rightarrow \bar{A} \rightarrow \bar{G} \rightarrow \bar{G}/\bar{A} \rightarrow \{1\}$$

ne sont pas scindées.

*Démonstration du théorème II.10.* — Supposons que l'une des deux suites (S) ou  $(\bar{S})$  soit scindée; alors la suite  $(\bar{S})$  est scindée. Puisque N contient A, la suite

$$\{1\} \rightarrow \bar{A} \rightarrow \bar{N} \rightarrow \bar{N}/\bar{A} \rightarrow \{1\}$$

est aussi scindée.

1° Nous allons en déduire l'assertion suivante :

« Il existe un sous-groupe L de  $\langle \mathcal{V}_{d-2} \rangle$ , stable par  $GL(\Omega)$ , et tel que

$$L \cdot \langle \mathcal{V}_{d-1} \rangle = \langle \mathcal{V}_{d-2} \rangle \quad \text{et} \quad L \cap \langle \mathcal{V}_{d-1} \rangle = \mathcal{O}(\Omega). »$$

[Autrement dit,  $\langle \mathcal{V}_{d-1} \rangle / \mathcal{O}(\Omega)$  est facteur direct de  $GL(\Omega)$ -module  $\langle \mathcal{V}_{d-2} \rangle / \mathcal{O}(\Omega)$ .]

Soit  $\pi$  la projection canonique de  $\bar{N}$  sur  $\bar{N}/\bar{A}$ . Selon l'hypothèse, il existe un morphisme  $\lambda$  de  $\bar{N}/\bar{A}$  dans  $\bar{N}$  et tel que  $\pi \circ \lambda = \text{Id}_{\bar{N}/\bar{A}}$ . Posons

$$K = \lambda(\bar{A} \cdot \bar{E} / \bar{A}).$$

On a

$$K \subset \pi^{-1}(\pi(K)) = \pi^{-1}(\bar{A} \cdot \bar{E}) \quad \text{soit} \quad K \subset \bar{A} \cdot \bar{E}$$

et

$$\bar{A} \cdot \bar{E} = \bar{A} \cdot K, \quad A \cap K = \{1\}.$$

Comme  $\bar{A} \cdot \bar{E} / \bar{A}$  est un sous-groupe distingué de  $\bar{N} / \bar{A}$ , K est distingué dans  $\lambda(\bar{N} / \bar{A})$ . En outre,  $\bar{A} \cdot \bar{E}$  étant abélien, K est également distingué dans  $\bar{A} \cdot \bar{E}$ . Au total, K est distingué dans  $\bar{A} \cdot \lambda(\bar{N} / \bar{A})$ , c'est-à-dire dans  $\bar{N}$ .

L'action de  $\bar{N}$  sur  $\bar{A} \cdot \bar{E}$  par automorphismes intérieurs définit dans  $\bar{A} \cdot \bar{E}$  une structure de  $GL(\Omega)$ -module sur  $\mathbf{F}_2$ , et  $\bar{A}$ ,  $\bar{\mathcal{C}}(\Omega)$  et K sont ainsi des

sous-modules de  $\overline{A} \cdot \overline{E}$ . Soit  $\rho$  la projection canonique de  $\overline{A} \cdot \overline{E}$  sur  $\overline{A} \cdot \overline{E} / \overline{\mathfrak{C}}(\Omega)$ . On a

$$\rho(\overline{A} \cdot \overline{E}) = \rho(\overline{A}) \cdot \rho(K)$$

et, comme  $\overline{\mathfrak{C}}(\Omega)$  est contenu dans  $\overline{A}$ ,

$$\rho(\overline{A}) \cap \rho(K) = \{1\}.$$

Le  $GL(\Omega)$ -module  $\overline{A} \cdot \overline{E} / \overline{\mathfrak{C}}(\Omega)$  est donc isomorphe à la somme directe de  $\rho(\overline{A})$  et de  $\rho(K)$ . Comme  $A = \mathfrak{C}(\Omega) \cdot E \langle \mathfrak{V}_{d-1} \rangle$  et  $E = E \langle \mathfrak{V}_{d-2} \rangle$ ,  $\overline{A} \cdot \overline{E} / \overline{\mathfrak{C}}(\Omega)$  est isomorphe comme  $GL(\Omega)$ -module à  $\langle \mathfrak{V}_{d-2} \rangle / \mathcal{O}(\Omega)$ . Dans cet isomorphisme,  $\overline{A} / \overline{\mathfrak{C}}(\Omega)$  s'envoie sur  $\langle \mathfrak{V}_{d-1} \rangle / \mathcal{O}(\Omega)$ . L'assertion est donc démontrée. Par ce même isomorphisme  $\rho(K)$  s'envoie sur un groupe de la forme  $L / \mathcal{O}(\Omega)$ , et le groupe  $L$  satisfait aux conditions de l'assertion 1.

2° Démontrons maintenant que  $L \cap \mathfrak{V}_{d-2}$  n'est pas vide.

Soit  $X$  un élément de  $\mathfrak{V}_{d-2}$ . Il existe  $H$  dans  $\mathfrak{V}_{d-1}$  tel que  $X \dot{+} H$  appartienne à  $L$ .

Si  $H = \emptyset$ , on a  $X \in (L \cap \mathfrak{V}_{d-2})$ . Supposons donc que  $H$  soit différent de  $\emptyset$ . Comme  $\mathcal{O}(\Omega)$  est contenu dans  $L$ , on peut supposer que  $H$  appartient à  $\mathfrak{V}_{d-1}$  (cf. la proposition I.8).

Si  $H$  est parallèle à  $X$  et contient  $X$ ,  $(X \dot{+} H)$  appartient à  $\mathfrak{V}_{d-2}$ . Si  $H$  est parallèle à  $X$  et ne contient pas  $X$ , on a cette fois-ci :

$$(X \dot{+} H \dot{+} \Omega) \in (L \cap \mathfrak{V}_{d-2}).$$

Supposons donc que  $H$  ne soit pas parallèle à  $X$ . Alors on a

$$(X \cap H) \in \mathfrak{V}_{d-3}.$$

Comme  $X \dot{+} H$  est le complément dans  $X \cup H$  de  $X \cap H$ ,  $X \dot{+} H$  est réunion disjointe de quatre variétés parallèles à  $X \cap H$  et de dimension  $d - 3$ . Alors, il existe nécessairement un hyperplan vectoriel  $\vec{H}'$  dans  $\Omega$  contenant trois d'entre ces variétés et non la quatrième <sup>(2)</sup>. Soit  $\sigma$  une transvection d'hyperplan  $H'$ . Il est clair que l'ensemble

$$Y = (X \dot{+} H) \dot{+} \sigma(X \dot{+} H)$$

---

<sup>(2)</sup> L'ensemble des variétés linéaires de dimension  $d - 3$  et parallèles à  $X \cap H$  est en bijection avec l'ensemble des points du quotient de  $F^d$  par  $X \cap H$ , espace de dimension 3. Or, dans un tel espace, si quatre points ne sont pas coplanaires, parmi les quatre plans affines qu'ils définissent, il y a un (et d'ailleurs un seul) plan vectoriel.

est réunion de deux variétés linéaires disjointes et parallèles, de dimension  $d - 3$ . On a par conséquent :

$$Y \in (L \cap \mathcal{V}_{d-2})$$

et l'assertion 2 est ainsi démontrée.

3° L'assertion 2 nous fournit la contradiction cherchée :

Remarquons que toute orbite du groupe linéaire dans  $\mathcal{V}_{d-2}$  engendre  $\langle \mathcal{V}_{d-2} \rangle$  <sup>(3)</sup>. Donc si  $L \cap \mathcal{V}_{d-2}$  n'est pas vide,  $L$  contient  $\langle \mathcal{V}_{d-2} \rangle$ , ce qui contredit le choix de  $L$  selon l'assertion 1.

## APPENDICE

### STABILISATEUR D'UN ESPACE TOTALEMENT SINGULIER MAXIMAL

Désignons par  $p$  un nombre entier, par  $q$  une puissance de  $p$ , et par  $\mathbf{F}_q$  le corps à  $q$  éléments. Un entier  $d \geq 1$  étant donné, soit  $V$  un  $\mathbf{F}_q$ -espace vectoriel de dimension  $2d$  muni d'une forme quadratique non dégénérée  $Q$ . Nous supposons  $Q$  d'indice  $d$ . Notons

$$x.y = Q(x + y) - Q(x) - Q(y);$$

l'application  $(x, y) \rightarrow x.y$  est une forme bilinéaire non dégénérée sur  $V$ . Si  $W$  est un sous-espace de  $V$ , désignons par  $W^0$  son orthogonal; rappelons que l'espace  $V/W^0$  s'identifie canoniquement au dual de l'espace vectoriel  $W$ .

Soit  $F$  un sous-espace totalement singulier maximal de  $V$ . Si  $a$  est un entier compris entre 0 et  $d$ , nous désignons par  $S_a(F)$  l'ensemble des sous-espaces totalement singuliers maximaux de  $V$  dont l'intersection avec  $F$  est de dimension  $a$ .

**PROPOSITION I.** — *Soit  $F$  un sous-espace totalement singulier maximal de  $V$  et soit  $O_F$  le stabilisateur de  $F$  dans le groupe orthogonal de  $Q$ . Soit  $I_F$  le sous-groupe de  $O_F$  formé des isométries qui opèrent trivialement sur  $F$ .*

(1)  *$I_F$  est un groupe abélien  $p$ -élémentaire d'ordre  $q^{\frac{d(d-1)}{2}}$  qui opère régulièrement sur l'ensemble  $S_0(F)$  des sous-espaces singuliers de  $V$  supplémentaires de  $F$ .*

(2) *Si  $F'$  est un supplémentaire totalement singulier de  $F$ , et si  $O_{F, F'}$  est le stabilisateur dans le groupe orthogonal du couple  $(F, F')$ , alors  $O_{F, F'}$  est isomorphe à  $GL(F)$ , et*

$$O_F = O_{F, F'} \rtimes I_F.$$

---

<sup>(3)</sup> Il est clair que le groupe linéaire  $GL(\Omega)$  a deux orbites dans  $\mathcal{V}_\alpha$  (si  $0 \leq \alpha \leq d - 1$ ), à savoir  $\mathcal{V}_\alpha$  et  $(\mathcal{V}_\alpha - \vec{\mathcal{V}}_\alpha)$ ; on peut donc utiliser le corollaire 3 de la proposition I.6.

*Démonstration de la proposition 1 :*

(a)  $I_F$  opère trivialement dans  $F$ , donc opère trivialement par transposition dans le dual de  $F$ ; il en résulte, grâce à l'identification du dual de  $F$  avec  $V/F$ , que  $I_F$  opère trivialement dans  $V/F$ . Ce groupe  $I_F$  est donc abélien  $p$ -élémentaire, isomorphe à un sous-groupe du groupe additif des matrices carrées d'ordre  $d$  à coefficient dans  $\mathbf{F}_q$ .

(b) Choisissons un supplémentaire totalement singulier de  $F$ , noté  $F'$ . Choisissons aussi une base  $\{e_1, e_2, \dots, e_d\}$  de  $F$ . Puisque  $F'$  est isomorphe à  $V/F$ , il existe dans  $F'$  une base duale, c'est-à-dire une base  $\{e'_1, e'_2, \dots, e'_d\}$  telle que pour tous  $i$  et  $j$ ,  $e_i \cdot e'_j = \delta_{i,j}$ . Il est clair qu'alors il y a correspondances bijectives entre :

— d'une part, entre les sous-espaces totalement singuliers supplémentaires de  $F$  et les systèmes libres singuliers  $\{x_1, x_2, \dots, x_d\}$  qui ont même image modulo  $F$  que  $\{e'_1, e'_2, \dots, e'_d\}$ ;

— d'autre part entre ces systèmes  $\{x_1, x_2, \dots, x_d\}$  et les éléments de  $I_F$  : à  $f \in I_F$  on associe le système  $\{f(e'_1), f(e'_2), \dots, f(e'_d)\}$ .

Ces remarques nous permettent de conclure que le groupe  $I_F$  opère régulièrement sur  $S_0(F)$ .

(c) Soit  $O_{F, F'}$  le stabilisateur de  $F'$  dans  $O_F$ . On voit facilement que  $O_{F, F'}$  est isomorphe à  $GL(F)$ . Puisque  $I_F$  opère régulièrement sur  $S_0(F)$ , on a  $O_{F, F'} \cap I_F = \{1\}$ . D'autre part,  $I_F$  est, par sa définition, distingué dans  $O_F$ . On a donc

$$O_F = O_{F, F'} \rtimes I_F.$$

(d) Il nous reste à calculer l'ordre de  $I_F$ . Un élément  $f$  de  $I_F$  est déterminé par la donnée de  $\{f(e'_1), f(e'_2), \dots, f(e'_d)\}$ , ou encore par la donnée de  $\tilde{f}$ , isomorphisme de  $F'$  dans  $F$  défini par

$$f(e'_i) = e'_i + \tilde{f}(e'_i).$$

Il est immédiat de vérifier que pour que le système  $\{e'_1 + f(e'_1), e'_2 + f(e'_2), \dots, e'_d + f(e'_d)\}$  soit singulier (donc détermine un élément de  $I_F$ ), il est nécessaire et suffisant que  $\tilde{f}$  soit alternée, c'est-à-dire que  $e'_i \cdot \tilde{f}(e'_j) + e'_j \cdot \tilde{f}(e'_i) = 0$  et  $e'_i \cdot \tilde{f}(e'_i) = 0$  pour tous  $i$  et  $j$  entre 0 et  $d$ . L'ordre de  $I_F$  est donc égal au nombre de matrices carrées alternées, soit encore  $q^{\frac{d(d-1)}{2}}$ .

**PROPOSITION 2.** — *Soit  $F$  un sous-espace totalement singulier maximal de  $V$ . Pour tout entier  $a$  compris entre 0 et  $d$ , l'ensemble  $S_a(F)$  est une orbite selon  $I_F$ .*

*Démonstration de la proposition 2 :*

(a) Soit  $F'$  un élément de  $S_a(F)$ . Choisissons une base  $\{e_1, e_2, \dots, e_a\}$ , de  $F \cap F'$  que nous complétons par un système libre  $\{e_{a+1}, \dots, e_d\}$  de manière à obtenir une base de  $F$ . En utilisant le fait que, dans l'espace  $(F + F')/(F \cap F')$ ,  $F'/(F \cap F')$  s'identifie au dual de  $F/(F \cap F')$ , on voit facilement qu'il existe un système  $\{e'_{a+1}, \dots, e'_d\}$  tel que  $\{e_1, \dots, e_d, e'_{a+1}, \dots, e'_d\}$  soit une base de  $F + F'$  et  $\{e_1, \dots, e_a, e'_{a+1}, \dots, e'_d\}$  une base de  $F'$  et que, pour tous  $i$  et  $j$  compris entre  $a + 1$  et  $d$ ,

$$e_i \cdot e'_j = \delta_{i,j}.$$

(b) Il est clair alors que si  $F'_1$  et  $F'_2$  sont deux éléments de  $S_a(F)$ , en faisant pour chacun une construction semblable à celle exposée en (a), on peut déterminer une isométrie  $u$  de  $F + F'_1$  sur  $F + F'_2$  telle que

$$u(F'_1) = F'_2.$$

#### BIBLIOGRAPHIE

- [1] E. R. BERLEKAMPF, *Algebraic Coding Theory*, Mc Graw Hill, 1968.
- [2] M. BROUÉ, *Le réseau de Leech et le groupe de Conway (Thèse de 3<sup>e</sup> cycle, Paris, 1970)*.
- [3] M. BROUÉ et M. ENGUEHARD, *Une famille infinie de formes quadratiques entières; leurs groupes d'automorphismes (C. R. Acad. Sc., Paris, t. 274, série A, 1972, p. 19-22)*.
- [4] J. H. CONWAY, *A group of order 8 315 553 613 086 720 000 (Bull. London Math. Soc., vol. 1, 1969, p. 79-88)*.
- [5] O. T. O'MEARA, *Introduction to quadratic forms*, Springer Verlag, Berlin, 1963.
- [6] W. W. PETERSON, *Error correcting codes*, M. I. T. Press, Cambridge, 1961.
- [7] I. S. REED, *A class of multiple-error-correcting codes and the decoding scheme (I. E. E. E. Trans. Inform. Theory, IT-4, 1954, p. 38-49)*.
- [8] J. H. VAN LINT, *Coding Theory (Lecture Notes, n° 201, Springer Verlag, Berlin, 1971)*.

Michel BROUÉ,  
18, rue du Général-Pajol,  
77130 Montereau  
et Michel ENGUEHARD,  
54, rue de Montdauphin,  
77240 Cesson.

