

# SÉMINAIRE HENRI CARTAN

JEAN-PIERRE SERRE

**Formes bilinéaires symétriques entières à discriminant  $\pm 1$**

*Séminaire Henri Cartan*, tome 14 (1961-1962), exp. n° 14-15, p. 1-16

<[http://www.numdam.org/item?id=SHC\\_1961-1962\\_\\_14\\_\\_A9\\_0](http://www.numdam.org/item?id=SHC_1961-1962__14__A9_0)>

© Séminaire Henri Cartan

(Secrétariat mathématique, Paris), 1961-1962, tous droits réservés.

L'accès aux archives de la collection « Séminaire Henri Cartan » 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/>

FORMES BILINÉAIRES SYMÉTRIQUES ENTIÈRES À DISCRIMINANT  $\pm 1$   
 par Jean-Pierre SERRE

Il s'agit de résultats arithmétiques qui sont utiles en topologie différentielle. On a pris pour guide le résumé qu'en donne MILNOR (cf. [5], ainsi que [6]).

I. Preliminaires.

1. Définitions.

Soit  $n$  un entier  $\geq 0$ . On va étudier la catégorie  $S_n$  définie de la manière suivante :

Un objet  $E$  de  $S_n$  est un  $\mathbb{Z}$ -module libre de rang  $n$ , muni d'une forme bilinéaire symétrique  $E \times E \rightarrow \mathbb{Z}$ , notée  $(x, y) \rightarrow xy$ , telle que :

(i) L'application linéaire de  $E$  dans son dual  $E^*$  définie par la forme  $xy$  est un isomorphisme.

Cette condition équivaut à la suivante (cf. BOURBAKI, Algèbre, Chap. IX, § 2, prop. 3) :

(ii) Si  $(e_i)$  est une base de  $E$ , et si  $a_{ij} = e_i e_j$ , le déterminant de la matrice  $A = (a_{ij})$  est égal à  $\pm 1$ .

La notion d'isomorphisme de deux objets  $E, E' \in S_n$  se définit de façon évidente : on écrit alors  $E \simeq E'$ . Il est commode d'introduire aussi  $S = \bigcup S_n$ ,  $n = 0, 1, \dots$

Si  $E \in S_n$ , l'application  $x \rightarrow xx$  fait de  $E$  un module quadratique. Si  $(e_i)$  est une base de  $E$ , et si  $x = \sum x_i e_i$ , la forme quadratique  $f(x) = xx$  est donnée par la formule

$$\begin{aligned} f(x) &= \sum_{i,j} a_{ij} x_i x_j, \text{ avec } a_{ij} = e_i e_j \\ &= \sum_i a_{ii} x_i^2 + 2 \sum_{i < j} a_{ij} x_i x_j. \end{aligned}$$

Les coefficients de ses termes rectangles sont donc pairs. Le discriminant de  $f$

(i. e.  $\det(a_{ij})$ ) est égal à  $\pm 1$ . Changer la base  $(e_i)$  revient à remplacer la matrice  $A = (a_{ij})$  par  ${}^tBAB$ , avec  $B \in \underline{GL}(n, \underline{Z})$ . Du point de vue de la forme  $f$ , cela revient à effectuer sur les variables  $(x_i)$  la substitution linéaire de matrice  $B$ ; la forme obtenue est dite équivalente à la forme  $f$ .

## 2. Opérations sur S.

2.1. - Si  $E, E' \in S$ , la somme directe  $E \oplus E'$  et le produit tensoriel  $E \otimes E'$ , munis des formes bilinéaires définies dans BOURBAKI (Algèbre, chap. IX, § 1, n° 3 et n° 9), appartiennent à  $S$ ; il suffit en effet de vérifier la condition (i), ce qui est immédiat.

2.2. - Si  $E \in S$ , et si  $m$  est un entier  $\geq 0$ , la puissance extérieure  $m$ -ième  $\bigwedge^m E$  de  $E$ , munie de la forme bilinéaire définie dans BOURBAKI, locato, appartient à  $S$ .

## 3. Invariants.

3.1. - Si  $E \in S_n$ , l'entier  $n$  s'appelle le rang de  $E$ , et se note  $r(E)$ .

3.2. - Soit  $E \in S$ , et soit  $V = E \otimes \underline{R}$  le  $\underline{R}$ -espace vectoriel obtenu en étendant les scalaires de  $\underline{Z}$  à  $\underline{R}$ . La forme quadratique de  $V$  s'écrit sous la forme

$$\sum_{i=1}^s x_i^2 - \sum_{j=1}^t y_j^2 \quad \text{par rapport à une base convenable de } V; \text{ on sait que le couple}$$

$(s, t)$  ne dépend pas de la base choisie (c'est la signature de  $V$ , cf. BOURBAKI, Algèbre, Chap. IX, § 7, n° 2). L'entier  $\tau(E) = s - t$  est appelé l'indice de  $E$ .

On a

$$-r(E) \leq \tau(E) \leq r(E) \quad \text{et} \quad r(E) \equiv \tau(E) \pmod{2}.$$

Lorsque  $\tau(E) = \pm r(E)$ , on dit que  $E$  est défini (la forme quadratique correspondante a un signe constant); dans le cas contraire, on dit que  $E$  est indéfini.

3.3. - Le discriminant de  $E$  par rapport à une base  $(e_i)$  ne dépend pas du choix de cette base. On le note  $d(E)$ . Il est égal à  $\pm 1$ . (Définition invariante:  $d(E) = +1$  si  $\bigwedge^r E$  est défini positif,  $d(E) = -1$  si  $\bigwedge^r E$  est défini négatif, avec  $r = r(E)$ .)

Si  $V = E \otimes \underline{R}$  est de signature  $(s, t)$ , on voit tout de suite que le signe de

$d(E)$  est égal à  $(-1)^t$ . Comme  $d(E) = \pm 1$ , on en déduit la formule

$$d(E) = (-1)^{(r(E) - \tau(E))/2}.$$

3.4. - Soit  $E \in S$ . On dit que  $E$  est pair (ou de type II) si la forme quadratique associée à  $E$  ne prend que des valeurs paires; si  $A$  est la matrice définie par une base de  $E$ , il revient au même de dire que tous les termes diagonaux de  $A$  sont pairs.

Si  $E$  n'est pas pair, on dit que  $E$  est impair (ou de type I). [Dans la terminologie des formes quadratiques, le type I correspond aux formes "propres" ("eigentlich") et le type II aux formes "impropres" ("uneigentlich").]

3.5. - Soit  $E \in S$ , et soit  $\bar{E} = E/2E$  la réduction de  $E \pmod{2}$ . C'est un espace vectoriel sur le corps  $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ . Par passage au quotient, la forme  $xy$  définit sur  $\bar{E}$  une forme  $\overline{xy}$ , qui est encore symétrique, et de discriminant  $\pm 1 = 1$ . La forme quadratique associée  $\overline{x^2}$  est additive:  $(\overline{x} + \overline{y})^2 = \overline{x^2} + \overline{y^2}$ . C'est donc un élément du dual de  $\bar{E}$ . Mais, la forme bilinéaire  $\overline{xy}$  définit un isomorphisme de  $\bar{E}$  sur son dual. On en conclut qu'il existe un élément canonique  $\bar{u} \in \bar{E}$  tel que l'on ait

$$\overline{ux} = \overline{xx} \text{ pour tout } \overline{x} \in \bar{E}.$$

[Dans les applications topologiques,  $\bar{u}$  s'interprète comme une classe de Wu.]

Revenant à  $E$ , on voit donc qu'il existe  $u \in E$ , défini  $\pmod{2E}$ , tel que

$$ux \equiv xx \pmod{2}.$$

Considérons l'élément  $uu \in \mathbb{Z}$ . Si l'on remplace  $u$  par  $u + 2x$ ,  $uu$  est remplacé par

$$(u + 2x)(u + 2x) = uu + 4(ux + xx) \equiv uu \pmod{8}.$$

L'image de  $uu$  dans  $\mathbb{Z}/8\mathbb{Z}$  est donc un invariant de  $E$ ; on le note  $\sigma(E)$ . Si  $E$  est de type II, on peut prendre  $u = 0$ , et l'on a donc  $\sigma(E) = 0$ .

3.6. - Soit  $E = E_1 \oplus E_2$ . Pour que  $E$  soit de type II, il faut et il suffit que  $E_1$  et  $E_2$  le soient. On a :

$$\begin{aligned} r(E) &= r(E_1) + r(E_2), & \tau(E) &= \tau(E_1) + \tau(E_2) \\ \sigma(E) &= \sigma(E_1) + \sigma(E_2), & d(E) &= d(E_1) \cdot d(E_2). \end{aligned}$$

#### 4. Exemples.

4.1. - On note  $I_+$  (resp.  $I_-$ ) le  $\mathbb{Z}$ -module  $\mathbb{Z}$  muni de la forme bilinéaire  $xy$  (resp.  $-xy$ ) ; il correspond à la forme quadratique  $+x^2$  (resp.  $-x^2$ ) .

Si  $s$  et  $t$  sont deux entiers  $\geq 0$  , on note  $sI_+ \oplus tI_-$  la somme directe de  $s$  copies de  $I_+$  et de  $t$  copies de  $I_-$  ; la forme quadratique correspondante est  $\sum_{i=1}^s x_i^2 - \sum_{j=1}^t y_j^2$  . Les invariants de ce module sont les suivants :

$$r = s + t , \quad \tau = s - t , \quad d = (-1)^t , \quad \sigma \equiv s - t \pmod{8} .$$

A part le cas trivial où  $(s, t) = (0, 0)$  , le module  $sI_+ \oplus tI_-$  est de type I.

4.2. - On note  $U$  l'élément de  $S_2$  défini par la matrice  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  .

La forme quadratique associée est la forme  $2x_1 x_2$  :  $U$  est de type II. On a

$$r(U) = 2 , \quad \tau(U) = 0 , \quad d(U) = -1 , \quad \sigma(U) = 0 .$$

4.3. - Soit  $k$  un entier  $\geq 0$  , soit  $n = 4k$  , et soit  $V$  l'espace vectoriel  $\mathbb{Q}^n$  , muni de la forme bilinéaire standard  $\sum x_i y_i$  , correspondant à la matrice unité. Soit  $E_0$  le sous-groupe de  $V$  formé des points à coordonnées entières ; muni de la forme bilinéaire induite par celle de  $V$  ,  $E_0$  est un élément de  $S_n$  , isomorphe à  $n \cdot I_+$  . Soit  $E_1$  le sous-module de  $E_0$  formé des éléments  $x$  tels que  $xx \equiv 0 \pmod{2}$  , c'est-à-dire  $\sum x_i \equiv 0 \pmod{2}$  . On a  $(E_0 : E_1) = 2$  . Soit  $E$  le sous-module de  $V$  engendré par  $E_1$  et par  $e = (\frac{1}{2}, \dots, \frac{1}{2})$  . On a  $2e \in E_1$  (du fait que  $n \equiv 0 \pmod{4}$ ) et  $e \notin E_1$  , d'où  $(E : E_1) = 2$  . Pour qu'un élément  $x = (x_i)$  de  $V$  appartienne à  $E$  , il faut et il suffit que l'on ait

$$2x_i \in \mathbb{Z} , \quad x_i - x_j \in \mathbb{Z} , \quad \sum_{i=1}^n x_i \in 2\mathbb{Z} .$$

On a alors  $xe = \frac{1}{2} \sum x_i \in \mathbb{Z}$  ; comme  $ee = k$  , on en conclut que la forme  $xy$  prend sur  $E$  des valeurs entières. De plus, le fait que  $E_1$  ait le même indice dans  $E_0$  et dans  $E$  montre que le discriminant de  $E$  est égal à celui de  $E_0$  , c'est-à-dire à  $+1$  . Le module quadratique  $E$  est donc un élément de  $S_n = S_{4k}$  ; on le notera  $V_n$  . Lorsque  $k$  est pair (i. e. lorsque  $n \equiv 0 \pmod{8}$ ) ,  $ee = k$  est pair, et on en déduit que  $xx$  est pair pour tout  $x \in E$  ;  $V_n$  est donc de type II lorsque  $n \equiv 0 \pmod{8}$  . On a

$$r(V_{8m}) = 8m, \quad \tau(V_{8m}) = 8m, \quad \sigma(V_{8m}) = 0, \quad d(V_{8m}) = 1.$$

Le cas de  $V_8$  est particulièrement intéressant. Il y a 240 vecteurs  $x \in V_8$  tels que  $xx = 2$  : si  $(e_i)$  désigne la base canonique de  $\mathbb{Q}^n$ , ce sont les vecteurs :

$$\pm e_i \pm e_k \quad (i \neq k), \quad \frac{1}{2} \sum \varepsilon_i e_i, \quad \varepsilon_i = \pm 1, \quad \prod \varepsilon_i = 1.$$

Leurs produits scalaires mutuels sont entiers ; ils forment donc ce que l'on appelle en théorie des groupes de Lie un système de racines, et l'on montre facilement que c'est celui du groupe exceptionnel  $E_8$  (cf. WITT [8]) ; comme système simple de racines, on peut prendre :

$$e_i - e_{i+1} \quad (2 \leq i \leq 7), \quad e_7 + e_8, \quad \frac{1}{2}(e_1 + e_8) - \frac{1}{2}(e_2 + \dots + e_7).$$

Ces vecteurs forment une base de  $V_8$ .

[On peut prendre bien d'autres bases, par exemple :

$$e, \quad e_3 + e_4, \quad e_3 - e_2, \quad e_3 - e_4, \quad e_5 - e_4, \quad e_5 - e_6, \quad e_7 - e_6, \quad e_7 - e_8$$

ce qui conduit à la matrice donnée par MILNOR [5] :

$$V = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 \end{pmatrix}.$$

On laisse au lecteur le soin de démontrer directement que  $V$  est définie positive et que  $\det(V) = 1, \dots$  ]

Pour  $m \geq 2$ , les vecteurs de longueur 2 de  $V_{8m}$  sont les  $\pm e_i \pm e_k$  ( $i \neq k$ ) ; ils forment un système de racines du type  $B_{8m}$ , cf. [8] ; noter qu'ils n'engendrent pas  $V_{8m}$ , contrairement à ce qui se passe dans le cas  $m = 1$ . En particulier,  $V_8 \oplus V_8$  n'est pas isomorphe à  $V_{16}$ .

## 5. Le groupe $K(S)$ .

C'est le groupe de Grothendieck de  $S$  : par définition, c'est le quotient du groupe abélien libre engendré par des éléments  $(E)$  correspondant aux  $E \in S$  par le sous-groupe engendré par les

$$(E) - (E_1) - (E_2) , \text{ pour } E \simeq E_1 \oplus E_2 .$$

En particulier, on a  $(E) = (E')$  dans  $K(S)$  s'il existe un  $F \in S$  tel que  $E \oplus F \simeq E' \oplus F$ . On verra plus loin (coroll. du th. 4) que réciproquement, si  $(E) = (E')$ , on a  $E \oplus F \simeq E' \oplus F$  avec  $F = I_+$  ou  $F = I_-$ .

Soit  $G$  un groupe abélien, et soit  $f : S \rightarrow G$  une application telle que  $f(E) = f(E_1) + f(E_2)$  si  $E \simeq E_1 \oplus E_2$ . On associe à  $f$  un homomorphisme (noté encore  $f$ ) de  $K(S)$  dans  $G$  tel que le composé  $S \rightarrow K(S) \rightarrow G$  soit l'application donnée.

[  $K(S)$  "représente" un foncteur dans la catégorie des groupes abéliens que le lecteur explicitera. ] En particulier,  $r, \tau, d, \sigma$  définissent des homomorphismes

$$r : K(S) \rightarrow \mathbb{Z} , \quad \tau : K(S) \rightarrow \mathbb{Z} , \quad d : K(S) \rightarrow \{\pm 1\} , \quad \sigma : K(S) \rightarrow \mathbb{Z}/8\mathbb{Z} .$$

On a ici encore  $\tau \equiv r \pmod{2}$ ,  $d = (-1)^{(r-\tau)/2}$ .

### Remarques.

1. Les opérations  $E \otimes E'$  et  $\bigwedge^m E$  permettent de munir  $K(S)$  d'une structure de  $\lambda$ -anneau, au sens de GROTHENDIECK.

2. La catégorie  $S$  peut se définir pour un anneau commutatif quelconque (et même en fait pour un schéma de base quelconque, non nécessairement affine) ; un élément de  $S$  est l'analogue algébrique d'un fibré vectoriel ayant pour groupe structural le groupe orthogonal. L'anneau  $K(S)$  correspondant remplace avantageusement l'anneau de Witt défini dans [7].

## II. Énoncé des résultats.

### 6. Détermination du groupe $K(S)$ .

THÉOREME 1. - Le groupe  $K(S)$  admet pour base  $(I_+)$  et  $(I_-)$  .

(La démonstration sera donnée au n° 13.)

En d'autres termes, tout  $f \in K(S)$  s'écrit de façon unique sous la forme

$$f = s.(I_+) + t.(I_-) , \text{ avec } s, t \in \underline{\mathbb{Z}} .$$

On a  $r(f) = s + t$ ,  $\tau(f) = s - t$ , ce qui montre que  $s$  et  $t$  sont déterminés par  $r$  et  $\tau$ . On en conclut :

COROLLAIRE 1. - Le couple  $(r, \tau)$  définit un isomorphisme de  $K(S)$  sur le sous-groupe de  $\underline{\mathbb{Z}} \times \underline{\mathbb{Z}}$  formé des éléments  $(a, b)$  tels que  $a \equiv b \pmod{2}$ .

D'où :

COROLLAIRE 2. - Pour que deux éléments  $E$  et  $E'$  de  $S$  définissent le même élément de  $K(S)$ , il faut et il suffit qu'ils aient même rang et même indice.

[Noter que cela n'entraîne nullement  $E \sim E'$ . Par exemple  $U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  définit dans  $K(S)$  le même élément que  $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = I_+ \oplus I_-$ , bien que  $U$  et  $I_+ \oplus I_-$  soient de types différents.]

THÉORÈME 2. - On a  $\sigma(E) \equiv \tau(E) \pmod{8}$  pour tout  $E \in S$ .

En effet,  $\tau$ , réduit mod 8, et  $\sigma$  sont des homomorphismes de  $K(S)$  dans  $\underline{\mathbb{Z}}/8\underline{\mathbb{Z}}$  qui coïncident sur les générateurs  $I_+$  et  $I_-$  de  $K(S)$ ; ils coïncident donc sur tout  $K(S)$ .

COROLLAIRE 1. - Si  $E$  est de type II, on a  $\tau(E) \equiv 0 \pmod{8}$ .

En effet  $\sigma(E) = 0$ .

(Noter que ceci entraîne  $r(E) \equiv 0 \pmod{2}$  et  $d(E) = (-1)^{r(E)/2}$ .)

COROLLAIRE 2. - Si  $E$  est défini et de type II, on a  $r(E) \equiv 0 \pmod{8}$ .

En effet, on a alors  $\tau(E) = \pm r(E)$ .

#### Remarques.

1. Inversement, on a vu au n° 4 que, pour tout  $n$  multiple de 8, il existe un  $E \in S_n$  qui est défini et de type II.

2. Pour une autre démonstration de la congruence  $\sigma \equiv \tau \pmod{8}$ , voir Van der BLIJ [1]. La congruence plus faible  $\sigma \equiv \tau \pmod{4}$  avait été rencontrée à propos d'un problème de topologie par HIRZEBRUCH et HOPF [2].

### 7. Théorèmes de structure (cas indéfini).

Soit  $E \in S$ . Nous dirons que  $E$  représente zéro s'il existe  $x \in E$ ,  $x \neq 0$ , tel que  $xx = 0$ .

THÉORÈME 3. - Si  $E \in S$  est indéfini,  $E$  représente zéro.

(La démonstration sera donnée au n° 11.)

THÉORÈME 4. - Si  $E \in S$  est indéfini et de type I,  $E$  est isomorphe à  $sI_+ \oplus tI_-$ , où  $s$  et  $t$  sont des entiers  $\geq 1$ .

[La forme quadratique correspondante est donc équivalente à la forme

$$\sum_{i=1}^s x_i^2 - \sum_{j=1}^t y_j^2 .]$$

(La démonstration sera donnée au n° 12.)

COROLLAIRE. - Soient  $E$  et  $E'$  deux éléments de  $S$  de même rang et de même indice. On a alors

$$E \oplus I_+ \simeq E' \oplus I_+ \quad \text{ou} \quad E \oplus I_- \simeq E' \oplus I_- .$$

C'est clair si  $E = 0$ . Sinon, l'un des deux modules  $E \oplus I_+$ ,  $E \oplus I_-$  est indéfini. Supposons que ce soit le premier. Comme  $E$  et  $E'$  ont même signature,  $E' \oplus I_+$  est également indéfini. En appliquant le théorème 4, on voit que  $E \oplus I_+$  et  $E' \oplus I_+$  sont isomorphes à  $sI_+ \oplus tI_-$  et  $s'I_+ \oplus t'I_-$  respectivement. Comme  $E$  et  $E'$  ont même signature, on a  $s = s'$ ,  $t = t'$ , d'où le résultat cherché.

THÉORÈME 5. - Si  $E \in S$  est indéfini, de type II, et si  $\tau(E) \geq 0$ ,  $E$  est isomorphe à  $pU \oplus qV_8$ , où  $p$  et  $q$  sont des entiers  $\geq 0$  convenables.

[Lorsque  $\tau(E) \leq 0$ , on a un résultat correspondant, obtenu en appliquant le théorème au module  $E^- = I_- \otimes E$ .]

(La démonstration sera donnée au n° 14.)

On notera que  $q = \frac{1}{8} \tau(E)$  et  $p = \frac{1}{2}(r(E) - \tau(E))$ . Il en résulte que  $E$  est déterminé à un isomorphisme près par son rang et son indice. Comme il en est de même pour le type I (cf. théorème 4), on peut énoncer :

THÉORÈME 6. - Si  $E$ ,  $E' \in S$  sont indéfinis, ont même rang, même indice, et même type, ils sont isomorphes.

### 8. Le cas défini.

On n'a pas de théorème de structure. On peut simplement affirmer que, pour chaque entier  $n$ ,  $S_n$  ne contient qu'un nombre fini de classes ; cela résulte par exemple du théorème de réduction donné au n° 10. La détermination explicite de ces classes n'a été faite que pour les petites valeurs de  $n$  ( $n \leq 16$ , cf. M. KNESER [4]).

Pour le type II, c'est particulièrement simple :

si  $r = 8$ ,  $V_8$  est la seule classe définie positive ,

si  $r = 16$ ,  $V_{16}$  et  $V_8 \oplus V_8$  sont les seules classes définies positives .

Ensuite, cela se complique : WITT affirme dans [8] avoir trouvé plus d'une dizaine de classes différentes de rang 24.

### III. Démonstrations.

#### 9. Un lemme.

Soit  $E \in S$ , et soit  $F$  un sous-module de  $E$  ; soit  $F'$  l'ensemble des  $x \in E$  orthogonaux aux éléments de  $F$ .

LEMME 1. - Pour que  $F$ , muni de la forme  $xy$  induite par celle de  $E$ , appartienne à  $S$ , il faut et il suffit que  $E$  soit somme directe de  $F$  et de  $F'$ .

Si  $E = F \oplus F'$ , on a  $d(E) = d(F) \cdot d(F')$ , d'où  $d(F) = \pm 1$ . Réciproquement, si  $d(F) = \pm 1$ , on a évidemment  $F \cap F' = 0$  ; de plus, si  $x \in E$ , la forme linéaire  $y \rightarrow x \cdot y$  ( $y \in F$ ) est définie par un élément  $x_0 \in F$ . On a alors  $x = x_0 + x_1$ , avec  $x_0 \in F$  et  $x_1 \in F'$ , d'où  $E = F \oplus F'$ .

COROLLAIRE. - Soit  $x \in E$  tel que  $xx = \pm 1$ , et soit  $X$  l'orthogonal de  $x$  dans  $E$ . Si  $D = \mathbb{Z}x$ , on a  $E = D \oplus X$ .

On applique le lemme 1 avec  $F = D$ .

[Si par exemple  $xx = +1$ , on a  $D \simeq I_+$ , d'où  $E \simeq I_+ \oplus X$ .]

#### 10. Réduction des formes quadratiques.

Soit  $V$  un  $\mathbb{Q}$ -espace vectoriel de dimension finie  $n$ , muni d'une forme bilinéaire symétrique non dégénérée, notée  $(x, y) \rightarrow xy$ . Soit  $E$  un réseau de  $V$ ,

c'est-à-dire un sous- $\mathbb{Z}$ -module de  $V$  de type fini tel que  $V = \mathbb{Q}.E$ . Si  $(e_i)$  est une base de  $E$ , le discriminant de la forme  $xy$  par rapport à  $(e_i)$  est indépendant du choix de  $(e_i)$ ; on le note  $d(E)$ ; c'est un élément de  $\mathbb{Q}^*$ .

Soit  $e_1$  le premier vecteur de la base  $(e_i)$ , et supposons que le nombre rationnel  $a_1 = e_1 e_1$  soit non nul. Soit  $V_1$  l'orthogonal de  $e_1$  dans  $V$ ; soit  $E_1$  l'image de  $E$  par la projection orthogonale  $V \rightarrow V_1$ . Il est clair que  $E_1$  est un réseau de  $V_1$ , admettant pour base les images  $\bar{e}_2, \dots, \bar{e}_n$  des  $e_i$ .

LEMME 2. - On a  $d(E_1) = (a_1)^{-1} d(E)$ .

Soit  $E' = \mathbb{Z}e_1 \oplus E_1$ . C'est un réseau de  $V$ , admettant pour base  $e_1, \bar{e}_2, \dots, \bar{e}_n$ . La matrice qui fait passer de la base  $(e_i)$  à la base précédente est triangulaire, et n'a que des 1 sur la diagonale; son déterminant est donc 1, ce qui montre que  $d(E') = d(E)$ . D'autre part, on a  $d(E') = d(\mathbb{Z}e_1) \cdot d(E_1)$ , et comme  $d(\mathbb{Z}e_1) = a_1$ , on obtient la formule voulue.

Soient encore  $V$  et  $E$  comme ci-dessus. Nous allons définir la notion de base réduite du réseau  $E$ . On procède par récurrence sur  $n$ . Si  $n \leq 1$ , toute base de  $E$  est dite réduite. Dans le cas général, une base  $(e_i)$  de  $V$  est dite réduite si elle vérifie les trois conditions suivantes :

- (i) Le scalaire  $a_1 = e_1 e_1$  est non nul; si  $x \in E$  est tel que  $xx \neq 0$ , on a  $|xx| \geq |a_1|$ .
- (ii) On a  $|e_1 e_i| \leq \frac{1}{2}|a_1|$  pour  $i \geq 2$ .
- (iii)  $(\bar{e}_2, \dots, \bar{e}_n)$  est une base réduite du réseau  $E_1$  de  $V_1$ .

On a

THÉOREME 7. - Tout réseau possède une base réduite.

On raisonne par récurrence sur  $n = \dim V$ , le cas  $n = 0$  étant trivial. Supposons  $n > 0$ . Parmi tous les  $x \in E$  tels que  $xx \neq 0$ , choisissons-en un, soit  $e_1$ , tel que  $e_1 e_1 = a_1$  soit minimum en valeur absolue (c'est possible, car les valeurs prises par la forme quadratique  $xx$  sur  $E$  sont des nombres rationnels à dénominateur borné). Il est clair que  $e_1$  est indivisible dans  $E$ , autrement dit fait partie d'une base de  $E$ . La donnée de  $e_1$  définit  $V_1$  et  $E_1$ . On choisit ensuite une base réduite  $(\bar{e}_2, \dots, \bar{e}_n)$  de  $E_1$ , ce qui est possible, vu l'hypothèse de récurrence; si  $e_i \in E$  se projette en  $\bar{e}_i$  sur  $E_1$ , les vecteurs  $(e_1, \dots, e_n)$  forment une base de  $E$  vérifiant évidemment les conditions (i) et (iii). De plus, on peut remplacer chaque  $e_i$  par  $e_i + k_i e_1$ , avec

$k_i \in \mathbb{Z}$  ; le produit scalaire  $e_1 e_i$  est alors remplacé par  $e_1 e_i + k_i a_1$  ; en choisissant convenablement  $k_i$ , on s'arrange pour que la condition (ii) soit vérifiée.

C. Q. F. D.

**THÉOREME 8.** - Si  $V$  ne représente pas zéro, et si  $(e_i)$  est une base réduite du réseau  $E$  de  $V$ , on a

$$|e_1 e_1| \leq \left(\frac{4}{3}\right)^{(n-1)/2} |d(E)|^{1/n}.$$

On raisonne par récurrence sur  $n$ , le cas  $n = 1$  étant trivial. On pose :

$$a_1 = e_1 e_1, \quad a_2 = e_2 e_2, \quad b = e_1 e_2, \quad c = \bar{e}_2 \bar{e}_2.$$

On a

$$|b| \leq \frac{1}{2}|a_1| \quad \text{et} \quad |a_2| \geq |a_1|$$

(car  $a_2 \neq 0$  vu l'hypothèse faite sur  $V$ ).

D'autre part, on a  $\bar{e}_2 = e_2 + ke_1$ , et  $e_1 \bar{e}_2 = 0$ , d'où  $k = -b/a_1$ . On en tire  $c = \bar{e}_2 \bar{e}_2 = a_2 + 2kb + k^2 a_1 = a_2 - b^2/a_1$ . D'où :

$$|c| \geq |a_1| - \frac{1}{4}|a_1|, \quad \text{c'est-à-dire} \quad |c| \geq \frac{3}{4}|a_1|.$$

Si l'on applique l'hypothèse de récurrence à  $E_1$ , on obtient l'inégalité

$$|c| \leq \left(\frac{4}{3}\right)^{(n-2)/2} |d(E_1)|^{1/(n-1)}$$

c'est-à-dire (lemme 2) :

$$|c| \leq \left(\frac{4}{3}\right)^{(n-2)/2} |a_1|^{-1/(n-1)} |d(E)|^{1/(n-1)}.$$

Comme  $|c| \geq \frac{3}{4}|a_1|$ , on trouve :

$$\frac{3}{4}|a_1| \leq \left(\frac{4}{3}\right)^{(n-2)/2} |a_1|^{-1/(n-1)} |d(E)|^{1/(n-1)},$$

ou encore :

$$|a_1|^{n/(n-1)} \leq \left(\frac{4}{3}\right)^{n/2} |d(E)|^{1/(n-1)},$$

c'est-à-dire

$$|a_1| \leq \left(\frac{4}{3}\right)^{(n-1)/2} |d(E)|^{1/n} .$$

C. Q. F. D.

**COROLLAIRE.** - Soit  $E \in S_n$ ,  $n \leq 5$ . Si  $E$  ne représente pas zéro,  $E$  est isomorphe à  $nI_+$  ou à  $nI_-$  (et en particulier  $E$  est défini).

On raisonne par récurrence sur  $n$ , le cas  $n \leq 1$  étant trivial. On pose  $V = E \otimes \mathbb{Q}$ , et l'on choisit une base réduite  $(e_i)$  de  $E$ , ce qui est possible d'après le théorème 7. Comme  $E$  ne représente pas 0, il en est de même de  $V$ ; comme  $|d(E)| = 1$ , le théorème 8 montre que

$$|e_1 e_1| \leq \left(\frac{4}{3}\right)^{(n-1)/2} < 2 \quad (\text{c'est ici que } n \leq 5 \text{ intervient}) .$$

Comme  $e_1 e_1$  appartient à  $\mathbb{Z}$ , ceci entraîne  $e_1 e_1 = \pm 1$ . Si, par exemple, on a  $e_1 e_1 = +1$ , le corollaire au lemme 1 montre que  $E \simeq I_+ \oplus E_1$ . L'hypothèse de récurrence, appliquée à  $E_1$ , montre que  $E_1 \simeq (n-1)I_+$  ou  $E_1 \simeq (n-1)I_-$ ; en fait, le second cas est exclu, car il entraînerait  $E \simeq I_+ \oplus (n-1)I_-$ , et  $E$  représenterait zéro. On a donc  $E \simeq nI_+$ .

C. Q. F. D.

### 11. Démonstration du théorème 3.

Rappelons d'abord un résultat classique sur les formes quadratiques à coefficients rationnels :

**THÉORÈME DE MEYER.** - Soit  $V$  un espace vectoriel quadratique non dégénéré sur  $\mathbb{Q}$ . Si  $V$  est indéfini et de dimension  $\geq 5$ ,  $V$  représente zéro.

On montre d'abord que l'hypothèse  $\dim V \geq 5$  entraîne que  $V \otimes \mathbb{Q}_p$  représente zéro pour tout nombre premier  $p$ ; d'autre part, puisque  $V$  est indéfini,  $V \otimes \mathbb{R}$  représente zéro. On en déduit que  $V$  lui-même représente zéro grâce au théorème de Hasse. Voir par exemple WITT [7] (qui traite le cas des corps de nombres), ou JONES [3] (qui se limite à  $\mathbb{Q}$ , mais donne des démonstrations "élémentaires").

Passons maintenant au théorème 3. Soit  $E \in S_n$ ,  $E$  indéfini. Si  $n \leq 5$ ,  $E$  représente zéro d'après le corollaire au théorème 8. Si  $n \geq 5$ ,  $E$  représente zéro d'après le théorème de Meyer.

C. Q. F. D.

## 12. Théorème de structure (cas indéfini impair).

(La méthode suivie ci-dessous m'a été indiquée par MILNOR.)

LEMME 3. - Soit  $E \in S_n$ . Supposons  $E$  indéfini et de type I. Il existe alors  $F \in S_{n-2}$  tel que

$$E \simeq I_+ \oplus I_- \oplus F .$$

D'après le théorème 3, il existe  $x \in E$ ,  $x \neq 0$ , tel que  $xx = 0$ ; quitte à diviser  $x$  par un entier, on peut supposer  $x$  indivisible. La forme linéaire  $y \rightarrow xy$  est alors un élément indivisible du dual  $E^*$  de  $E$ ; il existe donc un  $y \in E$  tel que  $xy = 1$ . On peut choisir  $y$  de telle sorte que  $yy$  soit impair. En effet, supposons que  $yy$  soit pair; puisque  $E$  est de type I, il existe  $t \in E$  tel que  $tt$  soit impair. Posons  $y' = t + ky$ , et choisissons  $k$  de telle sorte que  $xy' = 1$ , i. e.  $k = 1 - xt$ ; on a  $y'y' \equiv tt \pmod{2}$ , et  $y'y'$  est impair. On peut donc supposer que  $yy = 2m + 1$ . Posons alors

$$e_1 = y - mx, \quad e_2 = y - (m + 1)x .$$

On constate immédiatement que  $e_1 e_1 = 1$ ,  $e_1 e_2 = 0$ ,  $e_2 e_2 = -1$ . Le sous-module  $G$  de  $E$  engendré par  $(e_1, e_2)$  est isomorphe à  $I_+ \oplus I_-$ ; d'après le lemme 1, on a donc  $E \simeq I_+ \oplus I_- \oplus F$ .

C. Q. F. D.

Démonstration du théorème 4. - On raisonne par récurrence sur  $n$ . Soit  $E \in S_n$ , avec  $E$  indéfini et de type I. D'après le lemme 3,  $E \simeq I_+ \oplus I_- \oplus F$ . Si  $n = 2$ , on a  $F = 0$ , et le théorème est démontré. Si  $n > 2$ , on a  $F \neq 0$ , et l'un des modules  $I_+ \oplus F$ ,  $I_- \oplus F$  est indéfini; supposons par exemple que ce soit le premier. Comme  $I_+$  est de type I, il en est de même de  $I_+ \oplus F$ , et l'hypothèse de récurrence montre que  $I_+ \oplus F$  est de la forme  $aI_+ \oplus bI_-$ ; d'où

$$E \simeq aI_+ \oplus (b + 1) I_- .$$

C. Q. F. D.

## 13. Détermination du groupe $K(S)$ .

Soit  $E \in S$ ,  $E \neq 0$ . Alors  $E \oplus I_+$  ou  $E \oplus I_-$  est indéfini et de type I. Appliquant le théorème 4, on en déduit que l'image de  $E$  dans  $K(S)$  est

combinaison linéaire de  $(I_+)$  et de  $(I_-)$ . Il s'ensuit que  $(I_+)$  et  $(I_-)$  engendrent  $K(S)$ . Comme leurs images par l'homomorphisme

$$(r, \tau) : K(S) \rightarrow \mathbb{Z} \times \mathbb{Z}$$

sont linéairement indépendantes,  $(I_+)$  et  $(I_-)$  forment une base de  $K(S)$ .

#### 14. Théorème de structure (cas indéfini pair).

LEMME 4. - Soit  $E \in S$ . Supposons  $E$  indéfini et de type II. Il existe alors  $F \in S$  tel que  $E \cong U \oplus F$ .

On procède comme dans la démonstration du lemme 3. On choisit d'abord un  $x \in E$ ,  $x \neq 0$ ,  $x$  indivisible, tel que  $xx = 0$ ; on choisit ensuite un  $y \in E$  tel que  $xy = 1$ . Si  $yy = 2m$ , on remplace  $y$  par  $y - mx$  et l'on obtient un nouvel  $y$  tel que  $yy = 0$ . Le sous-module  $G$  de  $E$  engendré par  $(x, y)$  est alors isomorphe à  $U$ ; d'après le lemme 1, on a  $E \cong U \oplus F$ .

C. Q. F. D.

LEMME 5. - Soient  $F_1, F_2 \in S$ . Supposons que  $F_1$  et  $F_2$  soient de type II, et que  $I_+ \oplus I_- \oplus F_1 \cong I_+ \oplus I_- \oplus F_2$ . Alors  $U \oplus F_1 \cong U \oplus F_2$ .

Pour simplifier les notations, on posera  $W = I_+ \oplus I_-$ ,  $E_i = W \oplus F_i$ ,  $V_i = E_i \otimes \mathbb{Q}$ . Dans  $E_i$ , soit  $E_i^0$  le sous-groupe formé des éléments  $x$  tels que  $xx \equiv 0 \pmod{2}$ ; c'est un sous-groupe d'indice 2 de  $E_i$ . On voit tout de suite qu'en fait  $E_i^0 = W^0 \oplus F_i$ , où  $W^0$  est l'ensemble des éléments  $x = (x_1, x_2)$  de  $W$  tels que  $x_1 \equiv x_2 \pmod{2}$ . Soit  $E_i^+$  le "dual" de  $E_i^0$  dans  $V_i$ , c'est-à-dire l'ensemble des  $y \in V_i$  tels que  $xy \in \mathbb{Z}$  pour tout  $x \in E_i^0$ . Il est clair que  $E_i^+ = W^+ \oplus F_i$ , où  $W^+$  est l'ensemble des  $(x_1, x_2)$  tels que  $2x_1 \in \mathbb{Z}$ ,  $2x_2 \in \mathbb{Z}$ ,  $x_1 - x_2 \in \mathbb{Z}$ . On a  $E_i^0 \subset E_i \subset E_i^+$ , et le quotient  $E_i^+/E_i^0$  est isomorphe à  $W^+/W_0$ ; c'est un groupe de type  $(2, 2)$ . Il existe donc trois sous-groupes strictement compris entre  $E_i^0$  et  $E_i^+$ ; ils correspondent aux trois sous-groupes d'ordre 2 d'un groupe de type  $(2, 2)$ . L'un d'eux est  $E_i$  lui-même; les deux autres seront notés  $E_i'$  et  $E_i''$ . Ici encore, on a

$$E_i' = W' \oplus F_i, \quad E_i'' = W'' \oplus F_i,$$

où  $W'$  et  $W''$  sont définis de façon évidente. On constate immédiatement que  $W'$  et  $W''$  sont isomorphes à  $U$  (on peut par exemple prendre pour base de  $W'$

les vecteurs  $a = (\frac{1}{2}, \frac{1}{2})$ ,  $b = (1, -1)$ ; on a  $aa = bb = 0$ ,  $ab = 1$ ; pour  $W$  on prend  $(\frac{1}{2}, -\frac{1}{2})$  et  $(1, 1)$ . Soit alors  $f: W \oplus F_1 \rightarrow W \oplus F_2$  un isomorphisme. Il se prolonge en un isomorphisme de  $V_1$  sur  $V_2$ , qui applique  $E_1$  sur  $E_2$ , donc aussi  $E_1^0$  sur  $E_2^0$  et  $E_1^+$  sur  $E_2^+$  vu les définitions de ces sous-groupes. Il applique donc aussi  $(E_1^+, E_1^-)$  soit sur  $(E_2^+, E_2^-)$ , soit sur  $(E_2^-, E_2^+)$ . Comme  $E_1^+$  et  $E_1^-$  sont isomorphes à  $U \oplus F_1$ , on voit bien que  $U \oplus F_1 \cong U \oplus F_2$ .

C. Q. F. D.

Démonstration du théorème 5. - On va d'abord prouver que, si  $E_1, E_2 \in S$  sont indéfinis, de type II, et ont même rang et même indice, ils sont isomorphes.

D'après le lemme 4, on a  $E_1 = U \oplus F_1$ ,  $E_2 = U \oplus F_2$ ; il est clair que  $F_1$  et  $F_2$  sont de type II et ont même rang et même indice. Les modules  $I_+ \oplus I_- \oplus F_1$  et  $I_+ \oplus I_- \oplus F_2$  sont indéfinis, de type I, de même rang et de même indice. D'après le théorème 4, ils sont isomorphes. Appliquant le lemme 5, on voit alors que  $E_1$  et  $E_2$  sont isomorphes, ce qui démontre notre assertion.

Le théorème 5 est maintenant immédiat: si  $E$  est défini, de type II, et si  $\tau(E) \geq 0$ , on détermine des entiers  $p$  et  $q$  par les formules

$$q = \frac{1}{8} \tau(E), \quad p = \frac{1}{2}(r(E) - \tau(E)).$$

En appliquant le résultat ci-dessus aux modules  $E$  et  $pU \oplus qV_8$ , on voit que ces modules sont isomorphes.

C. Q. F. D.

## BIBLIOGRAPHIE

- [1] BLIJ (F. Van der). - An invariant of quadratic forms mod 8, Koninkl. nederl. Akad. van Wetensch., Series A, t. 62, 1959, p. 291-293.
- [2] HIRZEBRUCH (F.) und HOPF (H.). - Felder von Flächenelementen in 4-dimensionalen Mannigfaltigkeiten, Math. Annalen, t. 136, 1958, p. 156-172.
- [3] JONES (Burton W.). - The arithmetic theory of quadratic forms. - S. 1., Mathematical Association of America, 1950 (Carus mathematical Monographs, 10).
- [4] KNESER (Martin). - Klassenzahlen definiter quadratischer Formen, Arch. der Math., t. 8, 1957, p. 241-250.

- [5] MILNOR (John). - On simply connected 4-manifolds, Symposium internacional de topologia algebraica [1956. Mexico] ; p. 122-128. - Mexico, Universidad nacional autonomia, 1958.
  - [6] MILNOR (John). - A procedure for killing homotopy groups of differentiable manifolds, Proceedings of the third symposium in pure mathematics of the American mathematical Society : Differential geometry ; p. 39-55. - Providence, American mathematical Society, 1961 (Proc. Symp. in pure Math., 3).
  - [7] WITT (Ernst). - Theorie der quadratischen Formen in beliebigen Körpern, J. für die reine und angew. Math., t. 176, 1937, p. 31-44.
  - [8] WITT (Ernst). - Eine Identität zwischen Modulformen zweiten Grades, Abh. math. Sem. Univ. Hamb., t. 14, 1941, p. 323-337.
-