PUBLICATIONS DU DÉPARTEMENT DE MATHÉMATIQUES DE LYON

LEÏLA HENOUD
MAURICE FLAMANT

Extensions cycliques non ramifiées

Publications du Département de Mathématiques de Lyon, 1974, tome 11, fascicule 3
, p. 71-139

<http://www.numdam.org/item?id=PDML_1974__11_3_71_0>

Publications du
Département de
Mathématiques
Lyon 1974 t.11-3

EXTENSIONS CYCLIQUES NON RAMIFIEES

par Leïla HENOUD et Maurice FLAMANT.

SOMMAIRE

IV - ELEMENTS DE TRACE NULLE DANS UNE EXTENSION CYCLIQUE NON RAMIFIEE.

A - Cas des extensions cycliques du type d'Artin-Schreier.

B - Cas des extensions cycliques du type de Kummer.

I - *FORMES BILINEAIRES ET FORMES QUADRATIQUES.*

A - GENERALITES.

Soient A un anneau commutatif, P un A-module et $B : P \times P \longrightarrow A$ une forme bilinéaire symétrique. On désigne par $d_B : P \longrightarrow P^*$ l'application linéaire associée à B; cette application est définie par :

$$d_B(x)y = B(x,y) \quad \forall x,y \in P.$$

DEFINITION 1.1. - *On dit que la forme bilinéaire* B *est* non dégénérée *si et seulement si l'application linéaire associée* d_B *est un isomorphisme.*

Exemple. - Soit E une extension algébrique séparable et de degré fini d'un corps K. L'application Tr : $(x,y) \longmapsto Tr_{E/K}xy$ de $E \times E$ dans K est une forme bilinéaire non dégénérée (N. BOURBAKI, *Algèbre* chap. 4 et 5, § 10, n° 6, Prop.12).

DEFINITION 1.2. - *Soit* (P,B) *un* A*-module bilinéaire. Un sous-module* U *de* P *est dit* totalement isotrope *si* $U \subset U^{\perp}$, $U^{\perp}$ *désignant l'orthogonal de* U *relativement à la forme bilinéaire* B.

Un sous-module U de P est dit *fortement non isotrope* si l'application $d_{B|U \times U}$ définit un isomorphe de U sur son dual U^*.

PROPOSITION 1.1 . - *Soient* (P,B) *un* A-*module bilinéaire et* U *un sous-*A-*module fortement non isotrope de* P. *Alors* P *est somme directe orthogonale de* U *et de* $U^{\perp}$.

Comme la restriction de B à U×U est non dégénérée par hypothèse, l'application $d_{B|U\times U}$ est un isomorphisme de U sur son dual U^* . Par suite, pour tout $y \in P$, il existe un élément y_o et un seul de U tel que : $B(x,y) = B(x,y_o)$ $\forall x \in U$. L'élément $y-y_o$ appartient à $U^{\perp}$, ce qui prouve que P est somme directe orthogonale de U et $U^{\perp}$.

PROPOSITION 1.2. - *Soient* (P,B) *un* A-*module bilinéaire non dégénérée et* U *un facteur direct de* P. *Les propositions suivantes sont équivalentes :*

a- Le facteur direct U *est fortement non isotrope.*

b- Le facteur direct $U^{\perp}$ *est fortement non isotrope.*

c- Le A-*module* P *est somme directe orthogonale des sous-modules* U *et* $U^{\perp}$.

a $\Longrightarrow$ c , d'après la proposition 1.1.

Montrons que c $\Rightarrow$ a et que c $\Rightarrow$ b . Par hypothèse $P = U \perp U^{\perp}$; par suite : $(P,B) = (U,B_1) \perp (U^{\perp},B_2)$ avec $B_1 = B|U\times U$, $B_2 = B|U^{\perp}\times U^{\perp}$ et $d_B = d_{B_1} \oplus d_{B_2}$;

or, d_B étant un isomorphisme de P sur P^* , d_{B_1} est un isomorphisme de U sur U^* et d_{B_2} un isomorphisme de $U^{\perp}$ sur $(U^{\perp})^*$.

Montrons que b $\Rightarrow$ a .

LEMME. - *Soit* (P,B) *un* A*-module bilinéaire non dégénéré et* N *un facteur direct de* P; *alors* $N^{\perp\perp} = N$.

Soient N un facteur direct du A-module P et M un supplémentaire de N dans P. Soit x un élément de P ; à cet élément l'isomorphisme d_B associe une forme linéaire x^* . Considérons la forme linéaire x_1^* définie de la manière suivante :

$x_1^* = x^*$ sur N ,

$x_1^* = o$ sur M.

Il existe un élément x_1 de P et un seul tel que $d_B(x_1) = x_1^*$. Pour tout $y \in M$ on a $B(x_1,y) = d_B(x_1).y = x_1^*(y) = o$; donc $x_1 \in M^\perp$.

D'autre part : $(x^* - x_2^*)(N) = o$; donc $N \subset \mathrm{Ker}(x^* - x_1^*)$ et, par suite, $x - x_1 \in N^\perp$.

Finalement $x = x_1 + x_2$, $x_1 \in M^\perp$, $x_2 \in N^\perp$. Il en résulte que $P = N^\perp + M^\perp$; mais $N^\perp \cap M^\perp = P^\perp = 0$. Le A-module P est somme directe des deux sous-modules $N^\perp$ et $M^\perp$. Ainsi $P = N \oplus M = N^\perp \oplus M^\perp = N^{\perp\perp} \oplus M^{\perp\perp}$.

Or $N \subset N^{\perp\perp}$ et $M \subset M^{\perp\perp}$; donc $N = N^{\perp\perp}$ et $M = M^{\perp\perp}$.

Le facteur direct $U^\perp$ est fortement non isotrope et $(U^\perp)^\perp = U^{\perp\perp} = U$. Il résulte de la proposition 1.1 que P est somme directe de U et de son orthogonal $U^\perp$.

B - ESPACES HYPERBOLIQUES.

DEFINITION 1.3. - *On appelle* espace hyperbolique *tout A-module bilinéaire non dégénéré, qui se décompose en somme directe de deux sous-modules totalement isotropes.*

THEOREME 1.1. - *Soit* (M,B) *un A-module bilinéaire. Les propriétés suivantes sont équivalentes :*

a - (M,B) *est un espace hyperbolique ·*

b - *Il existe un A-module reflexif* N *tel que les A-modules bilinéaires* (M,B) *et* $(N \oplus N^*, B^N)$ *soient isomorphes.*

La forme bilinéaire B^N est définie par $B^N[(x,x'),(y,y')] = \langle x,y'\rangle + \langle y,x'\rangle$.

b $\Longrightarrow$ a . Il suffit évidemment de montrer que $(N \oplus N^*, B^N)$ est un espace hyperbolique. Comme $B^N[(x,o),(y,o)] = \langle x,o\rangle + \langle y,o\rangle = 0 \quad \forall x,y \in N$ et $B^N[(o,x'),(o,y')] = \langle o,x'\rangle + \langle 0,y'\rangle = 0 \quad \forall x',y' \in N^*$, les sous-modules N et N^* sont totalement isotropes.

Montrons enfin que la forme bilinéaire B^N est non dégénérée. Il suffit de s'assurer que l'application d_{B^N} est un isomorphisme de $N \oplus N^*$ sur $(N \oplus N^*)^*$ qui est canoniquement isomorphe à $N^* \oplus N^{**}$. En effet :

$$B^N[(x,x'),(y,y')] = [d_{B^N}(y,y')].(x,x') = \langle x,y'\rangle + \langle y,x'\rangle.$$

$$= \langle x,y' \rangle + \langle x', C_N(y) \rangle = \langle (x,x'),(y',C_N(y)) \rangle \ ;$$

donc $d_{B^N}(x,x') = (x',C_N(x))$; N étant un A-module réflexif, C_N est un isomorphisme. Il est alors immédiat de vérifier que d_{B^N} est un isomorphisme.

a $\Longrightarrow$ b . Soit $M = N \oplus P$ une décomposition du A-module M en somme directe de deux sous-modules N et P totalement isotropes. Si N° et P° désignent respectivement les orthogonaux de N et P dans M^*, alors $d_B(N) \subset N^\circ$ et $d_B(P) \subset P^\circ$. Or $M^* = N^\circ \oplus P^\circ$ et la forme bilinéaire B étant non dégénérée, l'application linéaire d_B induit des isomorphismes $h : N \to N^\circ$ et $g : P \to P^\circ$.

Désignons par $\phi : N^\circ \to P^*$ (resp. $\psi : P^\circ \to N$) l'isomorphisme canonique défini par $\phi(y) = y|P$ (resp. $\Psi(z) = z|N$).

Les applications composées $u = \phi \circ h$ et $v = \psi \circ g$ sont également des isomorphismes. Posons $w = ({}^t v)^{-1} = {}^t(v^{-1})$ et étudions l'isomorphisme $w \circ u : N \to N^{**}$.

Pour $x \in N$ et $x' \in N^*$, nous avons :

$$\begin{aligned}\langle x',(w \circ u).(x)\rangle &= \langle v^{-1}(x'),u(x)\rangle = \langle (0,v^{-1}(x'),h(x)\rangle \\ &= \langle (0,v^{-1}(x'),d_B(x,0)\rangle = \langle (x,0),d_B(0,v^{-1}(x'))\rangle \\ &= \langle (x,0),(g \circ v^{-1})(x')\rangle = \langle (x,0),\Psi^{-1}(x')\rangle = \langle x,x'\rangle\end{aligned}$$

Ce calcul permet d'affirmer que :

1) $w \circ u = C_N$,

2) $B[(x,0),(0,v^{-1}(y'))] = \langle x,y' \rangle$,

$B[(0,v^{-1}(x')),(y,0)] = \langle y,x' \rangle$.

Considérons alors l'isomorphisme $k : M = N \oplus P \to N \oplus N^*$ défini par $k(x,z) = (x,v(z))$, $x \in N$, $z \in P$.

Pour $X = (x,x')$ et $Y = (y,y')$ où $x,y \in N$ et $x',y' \in N^*$, il vient

$$B[k^{-1}(X),k^{-1}(Y)] = B[(x,v^{-1}(x')),(y,v^{-1}(y'))] =$$

$$B[(x,0)+(0,v^{-1}(x')),\ (y,0)+(0,v^{-1}(y'))] .$$

En utilisant le fait que les sous-modules N et P sont totalement isotropes, on obtient :

$$B[h^{-1}(X),k^{-1}(Y)] = B[(x,0),(0,v^{-1}(y'))] + B[(0,v^{-1}(x')),(y,0)] = \langle x,y'\rangle + \langle y,x'\rangle,$$

$$B_o(k^{-1} \times k^{-1}) = B^N.$$

Les A-modules bilinéaires (M,B) et $(N \oplus N^*, B^N)$ sont isomorphes.

Dans la suite, nous utiliserons certaines propriétés de la structure d'espace hyperbolique; pour une meilleure compréhension, nous les rappellerons avec leur démonstration.

Soit P un A-module réflexif, nous notons $\mathbb{H}(P)$ l'espace hyperbolique $(P \oplus P^*, B^P)$. Soit alors $f : P \to Q$ un isomorphisme de A-modules, considérons l'isomorphisme A-linéaire $\mathbb{H}(f) = f \oplus ({}^t f)^{-1}$ qui applique $\mathbb{H}(P)$ sur $\mathbb{H}(Q)$.

Nous avons de plus :

$$\begin{aligned} B^Q[\mathbb{H}(f)(x,x'),\mathbb{H}(f).(y,y')] &= \langle f(x),({}^t f)^{-1}(y')\rangle + \langle f(y),({}^t f)^{-1}(x')\rangle \\ &= \langle f^{-1}(f(x)),y'\rangle + \langle f^{-1}(f(y)),x'\rangle \\ &= \langle x,y'\rangle + \langle y,x'\rangle = B^P[(x,x'),(y,y')]. \end{aligned}$$

L'application $\mathbb{H}(f)$ est un isomorphisme de A-modules bilinéaires. Enfin :

$$\mathbb{H}(1_P) = 1_P \oplus ({}^t 1_P) = 1_P \oplus 1_{P^*} = 1_{P \oplus P^*}.$$

Pour des isomorphismes de A-modules $f : P \to Q$ et $g : Q \to R$, on a :

$$\mathbb{H}(g \circ f) = (g \circ f) \oplus [{}^t(g \circ f)]^{-1} = (g \circ f) \oplus [({}^t g)^{-1} \circ ({}^t f)^{-1}] = \mathbb{H}(g) \circ \mathbb{H}(f).$$

La correspondance $\mathbb{H}$ est un foncteur de la catégorie dont les objets sont les A-modules réflexifs et les morphismes, les isomorphismes de A-modules dans la catégorie dont les objets sont les A-modules bilinéaires non dégénérés et les morphismes, les isomorphismes de A-modules bilinéaires.

PROPOSITION 1.3. - *Soient* P_1 et P_2 *deux A-modules réflexifs. Il existe un isomorphisme canonique* ϕ *entre les A-modules bilinéaires* $\mathbb{H}(P_1) \perp \mathbb{H}(P_2)$ *et* $\mathbb{H}(P_1 \oplus P_2)$, *où*

$$\mathbb{H}(P_1) \perp \mathbb{H}(P_2) = [(P_1 \oplus P_1^*) \oplus (P_2 \oplus P_2^*), B^{P_1} \perp B^{P_2}],$$

$$\mathbb{H}(P_1 \oplus P_2) = [(P_1 \oplus P_2)^*, B^{P_1 \oplus P_2}].$$

Considérons l'application ϕ de $\mathbb{H}(P_1) \perp \mathbb{H}(P_2)$ dans $\mathbb{H}(P_1 \oplus P_2)$ définie de la manière suivante :

$$\Phi[(x_1+f_1)+(x_2+f_2)] = (x_1+x_2)+ f \ , \ x_1 \in P_1 \ , \ f_1 \in P_1^* \ , \ x_2 \in P_2 \ , \ f_2 \in P_2^* \ ,$$

où f est la forme A-linéaire sur $P_1 \oplus P_2$ telle que $f(z_1+z_2) = f_1(z_1)+ f_2(z_2)$, $z_1 \in P_1$, $z_2 \in P_2$. Il est facile de vérifier que ϕ est un isomorphisme. Enfin :

$$B^{P_1\oplus P_2}[\phi(x_1+f_1+x_2+f_2),\phi(y_1+g_1+y_2+g_2)] = B^{P_1\oplus P_2}(x_1+x_2+f,y_1+y_2+g)$$

$$= \langle x_1+x_2,g\rangle + \langle y_1+y_2,f\rangle,$$

$$= g_1(x_1)+g_2(x_2) + f_1(y_1) + f_2(y_2),$$

$$(B^{P_1} \perp B^{P_2})(x_1+f_1+x_2+f_2,y_1+g_1+y_2+g_2) = B^{P_1}(x_1+f_1,y_1+g_1) + B^{P_2}(x_2+f_2,y_2+g_2)$$

$$= g_1(x_1)+f_1(y_1)+g_2(x_2) + f_2(y_2) ;$$

donc $B^{P_1\oplus P_2} \circ (\phi \times \phi) = B^{P_1} \perp B^{P_2}$

PROPOSITION 1.4. - *Soient* A' *un anneau commutatif unitaire,* h : A$\longrightarrow$A' *un homomorphisme d'anneaux et* P *un* A*-module projectif de type fini. Il existe un isomorphisme canonique entre les* A'*-modules* $A' \otimes_A \mathbb{H}(P)$ *et* $\mathbb{H}(A' \otimes_A P)$.

Le A'-module $A' \otimes_A P$ est projectif et de type fini ; donc en particulier il est réflexif. L'espace hyperbolique $\mathbb{H}(A' \otimes_A P)$ est défini. Soient $g : A' \otimes_A (P \oplus P^*) \longrightarrow (A' \otimes_A P) \oplus (A' \otimes_A P^*)$ le A'-isomorphisme canonique défini par : $g'[a' \otimes (x+f)] = (a' \otimes f) + (a' \otimes f)$ $a' \in A$, $x \in P$, $f \in P^*$, et $v : A' \otimes_A P^* \longrightarrow \mathrm{Hom}_{A'}(A' \otimes_A P, A')$ le A'-isomorphisme canonique tel que $v(a' \otimes f)$ $(a' \in A', f \in P^*)$ soit la forme A'-linéaire $b' \otimes y \longmapsto a'b'h[f(y)]$ et $\theta : A' \otimes_A (P \oplus P^*) \longrightarrow (A' \otimes_A P) \oplus (A' \otimes_A P)$ le A'-isomorphisme $(1_{A' \otimes_A P} \oplus v) \circ g$.

Montrons que θ est un isomorphisme de A'-modules bilinéaires :

$$B^{A' \otimes_A P}[\theta(a'\otimes(x+f)),\theta(b'\otimes(y+g))] = B^{A' \otimes_A P}[a'\otimes x+v(a'\otimes f),\ b'\otimes y+v(b'\otimes g)]$$

$$= v(b'\otimes g).(a'\otimes x)+v'(a'\otimes f).(b'\otimes y)$$

$$= a'b'h[g(x)]+a'b'h[f(y)] = a'b'h[g(x)+f(y)].$$

Désignons par B' la forme bilinéaire obtenue à partir de B^P par extension des scalaires de A à A' relativement à l'homomorphisme h ; on a

$B'[a'\otimes(x+f),b'\otimes(y+g)] = a'b'h[B^P(x+f,y+g)] = a'b'h[g(x)+f(y)]$; donc

$B^{A'\otimes_A P}{}_{\circ}(\theta\times\theta) = B'$.

Supposons maintenant que l'anneau A soit noethérien et intégralement clos. Etant donné un A-module M de type fini, nous noterons C(M) la classe de diviseurs attachée à M(N. BOURBAKI, *Algèbre Commutative*, Ch. 7, § 4, n° 7).

THEOREME 1.2. - *Tout espace hyperbolique de type fini sur un anneau noethérien intégralement clos est de classe nulle.*

Nous démontrerons d'abord un lemme.

LEMME 1. - *Soit* A *un anneau noéthérien intégralement clos; alors, pour tout* A*-module* M *de type fini sans torsion,* $C(M^*) = -C(M)$.

Il existe un sous-module libre L de M et un idéal δ de A tels que la suite de A-modules $0 \longrightarrow L \xrightarrow{u} M \longrightarrow \delta \longrightarrow 0$ soit exacte (N. BOURBAKI. *Algèbre commutative*, chap. 7, § 4, n° 9, théorème 6).

Les A-modules L,M, δ étant de types finis : $C(M) = C(L)+C(\delta) = C(\delta)$.

Soit $\mathfrak{P}$ un idéal premier de hauteur $\leqslant 1$ dans A; la suite de $A_{\mathfrak{P}}$-modules

$0 \longrightarrow L_{\mathfrak{P}} \xrightarrow{u_{\mathfrak{P}}} M_{\mathfrak{P}} \longrightarrow \delta_{\mathfrak{P}} \longrightarrow 0$ est exacte et scindée, car $\delta_{\mathfrak{P}}$ est un $A_{\mathfrak{P}}$-module libre. Il s'ensuit que la suite de $A_{\mathfrak{P}}$-modules

$0 \longrightarrow \delta_{\mathfrak{P}} \longrightarrow M_{\mathfrak{P}} \xrightarrow{{}^t u_{\mathfrak{P}}} L_{\mathfrak{P}} \longrightarrow 0$ est également exacte et scindée. Ceci montre que $\mathrm{Coker}({}^t u)$ est un A-module pseudo-nul; donc $C(\mathrm{Coker}\,{}^t u) = 0$.

Considérons alors la suite exacte de A-modules

$0 \longrightarrow \delta^* \longrightarrow M^* \xrightarrow{{}^t u} L^* \longrightarrow \mathrm{Coker}\ {}^t u \longrightarrow 0.$

Il vient $-C(\delta^*) + C(M^*) = 0$; donc $C(M^*) = C(\delta^*)$. Or $C(\delta^*) = C(A:\delta) =$ $C(\mathrm{div}(A:\delta)) = C(\mathrm{div}A - \mathrm{div}\delta) = -C(\mathrm{div}\delta) = -C(\delta)$. Ainsi $C(M^*) = -C(M)$.

Soit M un espace hyperbolique sur un anneau noethérien intégralement clos. Il existe un A-module réflexif N tel que M soit isomorphe au A-module $N \oplus N^*$. Si de plus M est de type fini, on a $C(M) = C(N) + C(N^*) = 0$.

THEOREME 1.3. - *Tout espace hyperbolique de type fini sur un anneau de Dedekind est un A-module libre.*

Démontrons d'abord le lemme suivant :

LEMME 1. - *Soit A un anneau de Dedekind. Pour tout A-module M de type fini sans torsion, les propositions suivantes sont équivalentes :*

a - *Le* A-*module* M *est libre* .

b - C(M) = 0.

a $\Rightarrow$ b . Cf. N.. BOURBAKI, *Algèbre commutative* , chap. 7, § 4, n° 7, proposition 16.

b $\Rightarrow$ a . On sait que, pour tout A-module M sans torsion de type fini et de rang $n \geqslant 1$, il existe un idéal $\delta \neq 0$ de A tel que M soit isomorphe à la somme directe des A-modules A^{n-1} et δ . On a alors $0=C(M)=C(A^{n-1})+C(\delta) = C(\delta)$.

Or les propositions suivantes sont équivalentes :

$c(\delta) = C(\mathrm{div}\delta) = 0$;

div δ est un diviseur principal ;

il existe $x \in K^*$ tel que div δ = div Ax.

Il en résulte que $\widetilde{\delta} = Ax$; mais, A étant un anneau de Dedekind, $\delta = \widetilde{\delta} = Ax$, $x \in A^*$ et M est isomorphe au A-module $A^{n-1} \oplus Ax$ qui est libre.

Pour un espace hyperbolique M de type fini sur un anneau de Dedekind, on a C(M) = 0; M est donc un A-module libre.

PROPOSITION 1.5. - *Soient* P *un espace hyperbolique et* (M,B) *un* A*-module bilinéaire non dégénéré, projectif et de type fini; alors le* A*-module bilinéaire* $P \otimes_A M$ *est un espace hyperbolique.*

Revenons d'abord sur la notion de produit tensoriel de formes bilinéaires. Soit $((P_i,B_i))_{i\in I}$ une famille finie de m A-modules bilinéaires symétriques. L'application $(x_1,\dots,x_m;y_1,\dots,y_m) \longmapsto \prod_{i\in I} B_i(x_i,y_i)$ $(x_i,y_i\in P_i,\ i=1,\dots,m)$ est une application A-multilinéaire de $P_1\times\dots\times P_m\times P_1\times\dots\times P_m$ dans A et définit une forme bilinéaire symétrique B sur $(\otimes_{i\in I} P_i)\times(\otimes_{i\in I} P_i)$. Celle-ci est caractérisée par : $B(x_1\otimes\dots\otimes x_m, y_1\otimes\dots\otimes y_m) = \prod_{i\in I} B_i(x_i,y_i)$, $x_i,y_i\in P_i$. On dit que B est le produit tensoriel des formes B_i et on note $B = \otimes_{i\in I} B_i$.

L'application $d_{\otimes_{i\in I} B_i} : \otimes_{i\in I} P_i \longrightarrow (\otimes_{i\in I} P_i)^*$ est composée de l'application

$\otimes_{i\in I} d_{B_i} : \otimes_{i\in I} P_i \longrightarrow \otimes_{i\in I} P_i^*$ et de l'application canonique $\mu : \otimes_{i\in I} P_i^* \longrightarrow (\otimes_{i\in I} P_i)^*$.

Lorsque μ est un isomorphisme, il est clair que, si les A-modules bilinéaires (P_i,B_i) sont non dégénérés, il en est de même du A-module bilinéaire (P,B). Cette condition est réalisée en particulier lorsque les A-modules P_i sont projectifs et de type fini.

Considérons le produit tensoriel R des A-modules bilinéaires P et M; il existe des sous-modules totalement isotropes P_1 et P_2 tel que $P = P_1\oplus P_2$. On a alors $R = (P_1\otimes M)\oplus(P_2\otimes M)$. Montrons que $P_1\otimes M$ (resp. $P_2\otimes M$) est totalement isotrope. Soient $x = \sum_i x_i\otimes m_i$, $y = \sum_j x_j\otimes m_j$ des éléments de $P_1\otimes M$. On a

$B(x,y) = \sum_{i,j} B(x_i\otimes m_i, x_j\otimes m_j) = \sum_{ij} B_1(x_i,x_j)B_2(m_i,m_j) = 0$; d'où le résultat.

COROLLAIRE. - *Le produit tensoriel de m espaces hyperboliques projectifs et de types finis est un espace hyperbolique.*

C - INDICE.

Nous terminerons cette présentation de la théorie des formes bilinéaires en revenant sur la notion d'indice. Nous admettrons les résultats suivants dont on trouvera une démonstration dans : W. KLINGENBERG, Orthogonale Gruppen über Lokalen Ringen, *Amer. J. Math.*, 83 (1961).

PROPOSITION 1.6. - *Soient* A *un anneau local dans lequel* 2 *est inversible et* (M,B) *un* A*-module libre, de rang* n *et non dégénéré. Tout facteur direct totalement isotrope est contenu dans un facteur direct totalement isotrope et maximal.*

PROPOSITION 1.7. - *Soient* A *un anneau local, dans lequel* 2 *est inversible et* (M,B) *un* A*-module libre de rang* n *et non dégénéré.*

a- Tous les facteurs directs totalement isotropes maximaux ont le même rang r *et sont permutés transitivement par les automorphismes métriques de* (M,B).

b - $r \leqslant \left[\frac{n}{2}\right]$.

Le nombre r est appelé l'*indice* de la forme bilinéaire B.

Nous nous proposons de généraliser la proposition précédente dans le cas où A est un anneau de Prüfer.

Soient A un anneau de Prüfer dans lequel 2 est inversible, (M,B) un A-module bilinéaire projectif de rang n non dégénéré et (T) l'ensemble des facteurs directs totalement isotropes. Cet ensemble ordonné par inclusion est inductif ; en effet, toute chaîne de facteurs directs totalement isotropes est finie, les rangs formant une suite croissante d'entiers bornée par n. Ainsi tout facteur direct totalement isotrope est contenu dans un facteur direct totalement isotrope maximal.

PROPOSITION 1.8. - *Soient* A *un anneau de Prüfer dans lequel* 2 *est inversible et* (M,B) *un A-module bilinéaire projectif de rang* n *et non dégénéré* .

a- Tous les facteurs directs totalement isotropes maximaux ont le même rang r *et ce rang est égal à l'indice commune des formes bilinéaires* B_p *obtenues à partir de* B *par localisation relativement aux idéaux premiers de* A.

b - $r \leqslant [\frac{n}{2}]$.

Nous admettrons le lemme suivant facile à démontrer en utilisant les propriétés des anneaux de Prüfer.

LEMME. - *Soient* A *un anneau de Prüfer,* M *un* A*-module projectif de type fini. Les propositions suivantes sont équivalentes :*

a- Le sous A *-module* N *est facteur direct de* M.

b- Il existe un idéal premier $\wp$ *de* A *tel que les conditions suivantes soient satisfaites :*

1) Le sous-module N *est saturé pour la partie multiplicative* $S = A-\wp$.

2) Le sous-$A_\wp$ *-module* $N_\wp$ *est un facteur direct du* $A_\wp$ *-module* $M_\wp$.

Soient alors $\wp_1$ et $\wp_2$ deux idéaux premiers de l'anneau A. Les formes bilinéaires $B_{\wp_1}$ et $B_{\wp_2}$ obtenues à partir de B par extension des scalaires de A à $A_{\wp_2}$ sont non dégénérées ; soient $r_{\wp_1}$ et $r_{\wp_2}$ leurs indices respectifs. Montrons que $r_{\wp_1} = r_{\wp_2}$. Soit $N_{\wp_1}$ un facteur direct totalement isotrope maximal du $A_{\wp_1}$-module $M_{\wp_1}$. Le A-module $N_1=(i_A^{\wp_1})^{-1}(N_{\wp_1})$ est un facteur direct totalement isotrope de M, de rang $r_{\wp_1}$. On a donc $r_{\wp_1} \leqslant r_{\wp_2}$. On démontre de même, mais en partant cette fois d'un facteur direct totalement isotrope maximal $N_{\wp_2}$ du $A_{\wp_2}$-module $M_{\wp_2}$, que $r_{\wp_2} \leqslant r_{\wp_1}$. Finalement $r_{\wp_1} = r_{\wp_2}$; on désignera par r l'indice commun à toutes les formes bilinéaires localisées $B_\wp$.

Désignons par K le corps des fractions de l'anneau A.

Soient U un facteur direct totalement isotrope maximal du A-module bilinéaire (M,B) et q son rang.

Si l'on avait $q > r$, le sous-espace vectoriel $U_o = K \otimes_A U$ serait alors un sous-espace vectoriel du K-espace vectoriel $M_o = K \otimes_A M$ totalement isotrope de dimension q, ce qui est impossible ; donc $q \leqslant r$.

Si l'on avait $q < r$, le sous-espace vectoriel U_o serait alors un sous-espace vectoriel de M_o totalement isotrope de dimension q et, par suite, U_o serait contenu dans un sous-espace vectoriel V_o totalement isotrope maximal ; $(i_A^o)^{-1}(V_o) = V$ serait donc un facteur direct de M totalement isotrope contenant strictement U, ce qui serait en contradiction avec le caractère maximal de U. Finalement $q = r$.

DEFINITION 1.4. - *Soient* A *un anneau de Prüfer*, (M,B) *un* A*-module bilinéaire projectif de type fini et non dégénéré. On appelle* indice *de la forme* B *le rang commun des facteurs directs totalement isotropes maximaux.*

Les facteurs directs totalement isotropes maximaux ne sont pas nécessairement permutés par les automorphismes métriques (voir M. FLAMMANT cours de D.E.A., 1971-1972).

PROPOSITION 1.9. - *Soient* A *un anneau de Prüfer dans lequel 2 est inversible et* $(P,B) = (P_1,B_1) \otimes_A (P_2,B_2)$ *le produit tensoriel de deux*

A-modules bilinéaires non dégénérés, projectifs, de rangs n_1 *et* n_2 *et d'indices respectifs* r_1 *et* r_2. *L'indice du A-module bilinéaire* (P,B) *est au moins égal à* $r_1n_2 + r_2n_1 - 2r_1r_2$.

La proposition 1.8 autorise à supposer l'anneau A local.

Les A-modules bilinéaires (P_1,B_1) et (P_2,B_2) admettent des décompositions de Witt $P_1=(N_1 \oplus M_1)\perp R_1$, $P_2=(N_1 \oplus M_2)\perp R_2$, où les facteurs directs N_i et M_i sont des facteurs directs totalement isotropes maximaux. Soit alors V le facteur direct de $P_1 \otimes_A P_2$ défini par :

$V = (N_1 \otimes_A P_2) \oplus (R_1 \otimes_A N_2)$.

$x \in V \Longrightarrow x = \sum_i n_{1,i} \otimes e_{2,i} + \sum_j r_{1,j} \otimes n_{2,j}$ et $y \in V \Rightarrow y = \sum_k n_{1,k} \otimes e_{2,k} + \sum_h r_{1,h} \otimes n_{2,h}$,

$(e_{2,i})$ et $(n_{2,h})$ étant des bases de P_2 et de N_2.

On vérifie sans difficulté que $B(x,y) = 0$, V est donc un facteur direct totalement isotrope; on a de plus : $rg_A V = r_1n_2 + (n_1-2r_1)r_2 = r_1n_2+r_2n_1-2r_1r_2$.

COROLLAIRE 1. - *Soient* A *un anneau de Prüfer dans lequel 2 est inversible et* (P_i,B_i) $(i=1,\ldots,m)$ m *A-modules bilinéaires non dégénérés projectifs, de rangs respectifs* n_i *et d'indice maximum. Le A-module bilinéaire* $(P,B) = \bigotimes_{i=1}^{i=m} (P_i,B_i)$ *est un A-module d'indice maximum.*

Supposons d'abord les n_i impairs; nous ferons la démonstration par récurrence sur m.

Pour m=1,la proposition est trivialement vraie.

Supposons que la proposition soit vraie à l'ordre k-1 : le produit tensoriel B' des formes bilinéaires $N_1,\ldots,B_{k-1}$ est une forme bilinéaire d'indice maximum $\frac{n_1\cdots n_{k-1} - 1}{2}$. Posons $n' = n_1\cdots n_{k-1}$ et

$r' = \frac{n_1\cdots n_{k-1} - 1}{2} = \frac{n'-1}{2}$. Le produit tensoriel des formes B' et B_k est une forme bilinéaire d'indice au moins égal à $r_k n'+r'n_k-2r'r_k =$

$$\frac{n_k-1}{2}\, n' + \frac{n'-1}{2}\, n_k - 2\,\frac{n_k-1}{2}\cdot\frac{n'-1}{2} = \frac{n'n_k-1}{2}\, r .$$

D'où le résultat.

Si l'un au moins des n_i est pair, le résultat est une conséquence de la proposition 1.5.

Nous utiliserons enfin le résultat suivant que nous énonçons sans démonstration.

PROPOSITION 1.10. - *Soient* A *un anneau de Prüfer dans lequel 2 est inversible et*(M,B) *un* A*-module bilinéaire non dégénéré, projectif , de type fini, contenant un facteur direct* N *totalement isotrope. Alors il existe un facteur direct totalement isotrope* P *et un facteur direct fortement non isotrope* R *tels que* $M = (N \oplus P) \perp R$.

Une telle décomposition du A-module bilinéaire (M,B) est appelée *décomposition de Witt.*

D - CARACTERISTAITON DES FORMES BILINEAIRES NON DEGENERES SUR UN A-MODULE PROJECTIF DE RANG 1.

Soient A un anneau intègre et K son corps des fractions.

On désigne par J(A) le groupe des idéaux fractionnaires inversibles de K, par $\mathcal{J}(A)$ le groupe des classes d'idéaux fractionnaires inversibles et par $\mathcal{P}(A)$ le groupe des classes d'isomorphie des A-modules projectifs de rang 1. L'application surjective $Cl : J(A) \longrightarrow \mathcal{P}(A)$ permet d'identifier canoniquement $\mathcal{J}(A)$ et $\mathcal{P}(A)$. Soit $\mathfrak{a} \in J(A)$; à toute forme bilinéaire B sur $\mathfrak{a} \times \mathfrak{a}$ est associée canoniquement l'homomorphisme d_B de $\mathfrak{a}$ dans $\mathfrak{a}^*$ tel que : $B(x,y) = d_B(y)x \quad \forall x,y \in \mathfrak{a}$. L'isomorphisme composé des isomorphismes canoniques $\mathrm{Hom}_A(\mathfrak{a}, \mathfrak{a}^*) \longrightarrow \mathrm{Hom}_A(\mathfrak{a}, \mathfrak{a}^{-1})$ et $\mathrm{Hom}_A(\mathfrak{a}, \mathfrak{a}^{-1}) \longrightarrow \mathfrak{a}$ associe à d_B un élément λ_B de $\mathfrak{a}^{-2}$ tel que :

$B(x,y) = \lambda_B xy \quad \forall\, x,y \in \mathfrak{a}$.

PROPOSITION 1.11. - *Pour un A-module bilinéaire* $(\mathfrak{a},B)$ *, les propositions suivantes sont équivalentes :*

a- Le A-module bilinéaire $(\mathfrak{a},B)$ *est non dégénéré ·*

b- Il existe un élément v *de* K^* *et un élément* v_B *de A, inversible dans A, tels que* $\mathfrak{a}^{-2} = Av$, $\lambda_B = v_B v$.

a. $\Longrightarrow$ b . Le A-module bilinéaire $(\mathfrak{a}, B)$ est non dégénéré; donc d_B est un isomorphisme de $\mathfrak{a}$ sur son dual $\mathfrak{a}^*$. Il en résulte que $cl(\mathfrak{a}) = cl(\mathfrak{a}^*) = cl(\mathfrak{a}^{-1})$, d'où $cl(\mathfrak{a}^{-2}) = 0$; $\mathfrak{a}^{-1}$ est un idéal fractionnaire principal et il existe $v \in K^*$ tel que $\mathfrak{a}^{-2} = Av$. La constante λ_B se met sous la forme $\lambda_B = rv$, $r \in A$. Enfin la forme B étant inversible, λ_B admet un inverse qui appartient à $\mathfrak{a}^2 = Av^{-1}$; d'où $\lambda_B = rv$, r étant inversible dans A.

b $\Longrightarrow$ a est évident.

II - *EXTENSIONS CYCLIQUES.*

A - GENERALITES.

DEFINITION 2.1. - *On dit qu'une extension* E *d'un corps* K *est* cyclique *si elle est galoisienne et si son groupe de Galois sur* K *est cyclique.*

Exemple. - Toute extension quadratique séparable E d'un corps K est cyclique sur K. Le corps $\mathbf{F}_{q^n}$ est une extension cyclique de degré m du corps $\mathbf{F}_q$.

Dans la suite, on supposera que K est un corps de caractéristique différente de 2. Pour une extension cyclique E du corps K, on désignera par σ un élément générateur du groupe de Galois Γ de E sur K.

Nous rappellerons les deux résultats suivants :

PROPOSITION 2.1. - *Soit* E *une extension algébrique séparable de degré* n *du corps* K, *produit tensoriel d'extensions algébriques séparables* E_i *de* K *de degré* n_i . *La forme bilinéaire*

$Tr : (x,y) \longmapsto Tr_{E/K}\, xy$ *sur* E *est le produit tensoriel des formes bilinéaires* $Tr_i : (x,y) \longmapsto Tr_{E/K} xy$.

On trouvera une démonstration dans N. BOURBAKI, *Algèbre*, chap. III, § 9, n° 3 (1970).

PROPOSITION 2.2. - *Soit* E *une extension cyclique d'un corps* K. *Alors* E *est isomorphe au produit tensoriel d'extensions cycliques de* K *dont chacune a un degré égal à une puissance d'un nombre premier.*

B - EXTENSIONS CYCLIQUES DU TYPE D'ARTIN-SCHREIER.

Extensions cycliques du type d'Artin-Schreier simple (en abrégé extensions A.S.S.).

Les extensions de ce type sont caractérisées par le théorème suivant, dont on trouvera une démonstration dans P. RIBENBOÏM, *L'Arithmétique dans les corps*, Hermann (1972).

THEOREME 2.1. - *Soit* K *un corps de caractéristique* $p \neq 0$.

a- Toute extension cyclique E *de* K *de degré* p *admet un élément primitif* θ, *racine d'un polynôme irréductible de* $K[X]$ *de la forme* X^p-X-a.

b- Pour tout $a \in K^*$, *le polynôme* X^p-X-a *de* $K[X]$ *est ou irréductible ou le produit de* p *facteurs du premier degré. Dans le premier cas, le corps des racines* E *de ce polynôme est une extension cyclique de* K *de degré* p.

c- Pour deux polynômes X^p-X-a *et* X^p-X-b *de* $K[X]$, *les propositions suivantes sont équivalentes :*

1 - Les corps des racines de ces polynômes sont identiques.

2- Il existe $k \in \mathbb{Z}$, $1 \leqslant k \leqslant p-1$ *et* $c \in K$ *tel que* $b = ka + (c^p - c)$.

Pour une extension A.SS. admettant un élément primitif θ racine d'un polynôme $X^p - X - a$ de $K[X]$, nous désignerons par σ le générateur du groupe de Galois défini par $\sigma(\theta) = \theta + 1$. Il vient alors : $\sigma^{(h)}(\theta^k) = [\sigma^{(h)}(\theta)]^k =$

$(\theta+K)^k$ $(h = 1,2,\ldots,p)$, $T_{r_{E/K}}(\theta^k) = \theta^k + (\theta+1)^k + \ldots + (\theta+p-1)^k =$

$$= p\theta^k + \sum_{i=1}^{i=k} C_k^i S_i(p)\theta^{k-1} = \sum_{i=1}^{i=k} C_k^i S_i(p)\theta^{k-1},$$

avec $S_i(p) = 1^i + 2^i + \ldots + (p-1)^i$.

Or nous savons que :

$S_i(p) \equiv 0 \pmod{p}$, si i n'est pas divisible par p-1;

$S_i(p) \equiv -1 \pmod{p}$, si i est divisible par p-1.

Il en résulte que :

$Tr_{E/K}(\theta^h) = 0 \quad (k=0,1,\ldots,p-2)$; $\quad Tr_{E/K}\theta^{p-1} = -1$;

$Tr_{E'K}(\theta^p) = Tr_{E/K}(\theta+a) = 0$;

$Tr_{E/K}(\theta^{p+h}) = Tr_{E/K}(\theta^{k+1} + a\theta^k) = 0 \quad (k=1,2,\ldots,p-3)$;

$Tr_{E/K}(\theta^{2p-2}) = Tr_{E/K}(\theta^{p-1} + a\theta^{p-2}) = -1$;

$Tr_{E/K}(\theta^{2p-1}) = Tr_{E/K}(\theta^p + a\theta^{p-1}) = -a$.

PROPOSITION 2.3. - *Le K-espace vectoriel bilinéaire* (E,Tr) *est un espace vectoriel bilinéaire d'indice maximum.*

Posons p = 2s+1 et soit N le sous-espace vectoriel de E engendré par les vecteurs $1,\theta,\ldots,\theta^{s-1}$. $x \in N \Rightarrow x = \sum_{i=o}^{i=s-1} \alpha_i \theta^i$, $\alpha_i \in K$; d'où

$$x^2 = \sum_{i=o}^{i=s-1} \alpha_i^2 \theta^{2i} + \sum_{\substack{i,j=o \\ i \neq j}}^{i;j=s-1} \alpha_i \alpha_j \theta^{i+j} \quad .$$

On vérifie facilement en utilisant les relations précédentes que $Tr_{E/K} x^2 = 0$. Il en résulte que N est un sous-espace totalement isotrope de dimension s ; donc l'indice de (E,Tr) est égal à s.

PROPOSITION 2.4. - *Le groupe de Galois* Γ *de* E *sur* K *est un sous-groupe du groupe des rotations de la forme* Tr.

REMARQUE. - Les vecteurs

$v_1 = \theta + \theta^{2s-1}$, ..., $v_{s-1} = \theta^{s-1} + \theta^{s+1}$, $v_s = \theta^s$, $v_{s+1} = \theta - \theta^{2s-1}$, ..., $v_{2s-1} = \theta^{s-1} - \theta^{s+1}$,

$v_{2s} = \theta^{2s}$, $v_{2s+1} = \theta^{2s} - 1$ constituent une base orthogonale de E.

Extensions cycliques du type d'Artin-Schreier généralisé (en abrégé extensions A.S.G.).

Les extensions de ce type sont caractérisées par le théorème suivant :

THEOREME 2.2. - *Soient* K *un corps de caractéristique* $p > o$, E *une extension cyclique de degré* $q = p^e$ *du corps* K, σ *un automorphisme de* E *engendrant le groupe de Galois de* E *sur* K *et* F *le corps intermédiaire entre* K *et* E *de degré* $m=p^{e-1}$ *sur* K.
Alors il existe un élément θ *de* E, *racine d'un polynôme irréductible* X^p-X-a *de* $F[X]$ *tel que* $E = F(\theta) = K(\theta)$.

Soit E une extension ASG de K de degré p^e. On pose $p=2s+1$, $p^e=2s'+1$ et on désigne par F_i le corps intérmédiaire entre K et E de degré p^{e-1} ; alors $F_{i-1} = F_i(\theta_i) = K(\theta_i)$, où θ_i est une racine d'un polynôme irréductible X^p-X-a_i de $F_i[X]$.

Si N_i le sous-espace vectoriel engendré sur F_i par les vecteurs θ_i^j $(j=0,1,\ldots,s-1)$, il vient :

$$\dim_K N_i = \frac{p^{e-i+1} - p^{e-i}}{2} .$$

PROPOSITION 2.5. - *Le K-espace vectoriel bilinéaire* (E,Tr)*est un espace vectoriel bilinéaire d'indice maximum.*

Le corps E peut être considéré comme une extension A.S.S.de F_1 engendrée par la racine θ_1 du polynôme X^p-X-a_1 de $F_1[X]$. Le sous-espace vectoriel N_1 de E engendré par les vecteurs $1, \theta_1, \ldots, \theta_1^{s-1}$ sur F_1 a pour dimension $\frac{p^e-p^{e-1}}{2}$ sur K et il est totalement isotrope ; en effet, pour tout $x \in N_1$, on a $Tr_{E/K}x^2 = Tr_{F_1/K}(Tr_{E/F_1}x^2)=0$.

Déterminons $N_1^\perp$; nous avons $N_1^\perp = N_1 \perp N_1'$, avec $\dim_K N_1' = p^{e-1}$.

Le sous-espace vectoriel engendré par θ_1^s sur F_1 pour dimension p^{e-1} ; il est orthogonal à N_1 et $N_1 \cap F_1\theta_1^s = \{0\}$; donc $N_1' = F_1\theta_1^s$ et $N_1^\perp = N_1 \perp F_1\theta_1^s$.

D'une manière générale, supposons que nous ayons déterminé un sous-espace vectoriel M_k de E totalement isotrope tel que $M_k^\perp = M_k \perp F_k\theta_1^s \ldots \theta_k^s$.

Le corps F_k est une extension A.S.G. de K de degré p^{e-k}. En utilisant la méthode précédente, nous déterminons dans F_k un sous-espace vectoriel N_{k+1} totalement isotrope, c'est-à-dire tel que $Tr_{F_k/K}x^2=0 \quad \forall x \in N_{k+1}$.

Le sous-espace vectoriel $N_{k+1}\theta_1^s \ldots \theta_k^s$ est un sous-espace vectoriel de E totalement isotrope, car pour tout x de N_{k+1} nous avons :

$$Tr_{E/K}x^2\theta_1^{2s}\ldots\theta_k^{2s} = Tr_{F_1/K}\, x^2\theta_1^{2s}\ldots\theta_k^{2s}\,(Tr_{E/F_1}\,\theta_1^{2s}) = Tr_{F_1/K}(-x^2\theta_1^{2s}\ldots\theta_k^{2s})$$

$$= \mathrm{Tr}_{F_{k-1}/K}(-1)^{k-1}x^2\theta_k^{2s} = \mathrm{Tr}_{F_k/K}(-1)^{k-1}x^2(\mathrm{Tr}_{F_{k-1}/F_k}\theta_k^{2s})$$

$$= \mathrm{Tr}_{F_k/K}(-1)^k x^2 = 0.$$

Posons $M_{k+1} = M_k \perp N_{k+1}\theta_1^s \ldots \theta_k^s$. On a

$\dim_K M_{k+1} = \dim_K M_k + \dim_K N_{k+1} = \frac{p^e - p^{e-k}}{2} + \frac{p^{e-k} - p^{e-k-1}}{2} = \frac{p^e - p^{e-k-1}}{2}$. Donc

$M_{k+1}^{\perp} = M_{k+1} \perp F_{k+1}\theta_1^s \ldots \theta_{k+1}^s$.

Nous obtenons finalement un sous-espace vectoriel M_e totalement isotrope et de dimension sur K égale à $\frac{p^{e-1}}{2}$.

PROPOSITION 2.6. - *Le groupe de Galois* Γ *de* E *sur* K *est un sous-groupe du groupe des rotations de la forme* Tr.

Pour un générateur σ de Γ on a $\sigma^{(p^{e-1})}(\theta_1) = \theta_1 + 1$; d'où $(\det \sigma)^{p^{e-1}} = \det(\sigma^{p^{e-1}}) = 1$. Or p^{e-1} étant impair, il en résulte $\det \sigma = 1$.

C - EXTENSIONS CYCLIQUES DU TYPE DE KUMMER.

- *Extensions cycliques du type de Kummer simple (en abrégé extensions K.S.).*

Les extensions de ce type sont caractérisées par le théorème suivant,

dont on trouvera une démonstration dans P. RIBENBOÏM, *L'Arithmétique dans les corps*, Hermann (1972).

THEOREME 2.3. - *Soient* K *un corps de caractéristique* p, n *un entier non multiple de* p *et tel que* K *contienne le corps des racines n-ièmes de l'unité.*

a- Pour toute extension cyclique E *de* K *de degré* n, *il existe un polynôme irréductible de* $K[X]$ *de la forme* X^n-a *tel que* E *soit engendré par une racine quelconque* θ *de ce polynôme.*

b- Pour tout $a \in K^*$, *le corps des racines* E *du polynôme* X^n-a *est une extension cyclique de* K *engendrée par l'une quelconque des racines de* X^n-a *et le degré* d *de* E *sur* K *est un diviseur de* n.

c- Pour deux polynômes X^n-a *et* X^n-b, *les propositions suivantes sont équivalentes :*

1- Les corps des racines de ees polynômes sont identiques.

2- Il existe un entier $k \geq 1$ *premier avec* n *et tel que* $b \in a^k K^{*n}$.

Pour une extension K.S. admettant un élément primitif θ racine d'un polynôme X^n-a de $K[X]$, nous désignerons par σ le générateur du groupe de Galois défini par $\sigma(\theta) = \eta\theta$, où η désigne une racine primitive n-ème de l'unité. Il vient alors :

$$\sigma^{(h)}(\theta^i) = [\sigma^{(h)}(\theta)]^i = \eta^{ki}\theta^i \quad (k=1,\ldots,n \ ; \ i=0,1,\ldots,n-1) \ ,$$

$$Tr_{E/K}\theta^i = \theta^i+\ldots+\sigma^{(h)}(\theta^i)+\ldots+\sigma^{(n-1)}(\theta^i)=\theta^i(1+\eta^i+\ldots+\eta^{n-1})=\theta^i\,\frac{1-\eta^{n_i}}{1-\eta^i} = 0,$$

$$Tr_{E/K}\theta^n = na.$$

PROPOSITION 2.7. - *Soit* E *une extension cyclique* K.S. *de degré* n *de* K.

a- Si n = 2h+1 , *le* K*-espace vectoriel bilinéaire* (E,Tr) *a pour indice* h.

b- Si n = 2h *et* si -a *est un carré dans* K, *le* K*-espace vectoriel bilinéaire* (E,Tr) *est un espace hyperbolique.*

Si n = 2h *et si* -a *n'est pas un carré dans* K, *le* K*-espace vectoriel bilinéaire* (E,Tr) *a pour indice* h-1.

a- n = 2h+1.

Soit N le sous-espace vectoriel de E engendré par le système libre $\theta,\theta^2,\ldots,\theta^h$.

$$x \in N \implies x = \sum_{i=1}^{i=h} \alpha_i\theta^i \quad , \ \alpha_i \in K. \ \text{D'où} \quad Xx^2 = \sum_{i=1}^{i=h} \alpha_i^2\theta^{2i} + 2 \sum_{\substack{i,j=1 \\ i\neq j}}^{i,j=h} \alpha_i\alpha_j\theta^{i+j} \ .$$

On vérifie facilement en utilisant les relations précédentes que $Tr_{E/K}x^2=0$. Il en résulte que N est un sous-espace vectoriel totalement isotrope de dimension h.

b- n=2h.

Soit N le sous-espace vectoriel de E engendré par le système libre $\theta,\theta^2,\ldots,\theta^{h-1}$. On vérifie que ce sous-espace est totalement isotrope. L' orthogonal $N^\perp$ de N se met sous la forme $N^\perp = N \perp R$, où R est le sous-espace vectoriel de E engendré par les vecteurs 1 et θ^h. Une condition nécessaire et suffisante pour que l'indice de (E,Tr) soit égal à h est qu'il existe un vecteur z de E satisfaisant aux conditions suivantes :

$Z = \alpha_o 1+\alpha_h\theta^h+x$, $x \in N$, $\alpha_o\alpha_h \neq 0$, $Tr_{E/K}z^2=0$.

La dernière condition s'écrit : $n(\alpha_o^2+a\alpha_h^2)=0$; or n n'étant pas multiple de p, cette condition devient : $\alpha_o^2+a\alpha_h^2 = 0$. Il en résulte qu'une condition nécessaire et suffisante pour que E soit un espace hyperbolique est que -a soit un carré dans le corps K.

COROLLAIRE. - *Le sous-espace vectoriel bilinéaire* T *des éléments de trace nulle est un espace hyperbolique.*

On a $E = K.1 \perp T$; donc $T = (K.1)^\perp$.

Or $E = K\,1 \perp (N \oplus P)$, où N et P sont les sous-espaces vectoriels totalement isotropes engendrés respectivement par les systèmes libres suivants : $\theta,\ldots,\theta^{h-1}$; $\theta^{h+1},\ldots,\theta^{2h}$.

Extensions cycliques du type de Kummer généralisées (en abrégé extensions K.G.).

Les extensions de ce type sont caractérisées par le théorème suivant :

THEOREME 2.4. - *Soient* K *un corps de caractéristique* p, q *un nombre premier différent de* p *tel que* K *contienne les racines* q*-èmes de l'unité* E, *une extension cyclique de degré* q^e *du corps* K, σ *un automorphisme de* E *engendrant le groupe de Galois de* E *sur* K *et* F *le corps entre* K *et* E *de degré* $m=q^{e-1}$ *sur* K. *Alors il existe un élément* θ *de* E, *racine d'un polynôme irréductible* X^q-a *de* $F[X]$ *et tel que* $E=F(\theta)=K(\theta)$.

Soit E une extension K.G. de K de degré q^e. On pose $q = 2h+1$, $q^e=2h'+1$ et on désigne par F_i le corps intermédiaire entre K et E de degré q^{e-i} ; alors $F_{i-1}=K(\theta_i) = F_i(\theta_i)$, où θ_i est une racine d'un polynôme irréductible X^q-a_i de $F_i[X]$. Soit N_i le sous-espace vectoriel engendré sur F_i par les vecteurs θ_i^j , j=1,...,h ; il vient : $\dim_K N_i=hq^{e-i}=q^{e-i+1}$ $\dim_K N_i=hq^{e-i}=\frac{q^{e-i+1}-q^{e-i}}{2}$.

PROPOSITION 2.8. - *Le* K*-espace vectoriel bilinéaire* (E,Tr) *est un espace vectoriel bilinéaire d'indice maximum.*

Le corps E peut être considéré comme une extension K.S. de F_1 de degré égal à q, engendré par la racine θ_1 du polynôme X^q-a_1 de $F_1[X]$. L'étude précédente montre que le sous-espace N_1 est totalement isotrope ; en effet, pour tout $x \in N_1$, on a $Tr_{E/K}x^2 = Tr_{E/K}(Tr_{E/F_1}x^2) = 0$.

De plus : $\forall x\in N_1$, $\forall y\in F_1$ $Tr_{E/K}xy = Tr_{F_1/K}y(Tr_{E/F_1}x) = 0$.

Les sous-espaces vectoriels N_1 et F_1 sont orthogonaux. Enfin, il est clair que $N_1 \cap F_1 = \{0\}$. Un calcul élémentaire sur les dimensions montre que $N_1^{\perp} = N_1 \perp F_1$.

D'une manière générale, supposons que nous ayons déterminé un sous-espace vectoriel M_k de E totalement isotrope tel que $M_k^{\perp} = M_k \perp F_k$. Le corps F_k est une extension K.G. de K de degré q^{e-k}. En utilisant la méthode précédente, nous déterminons dans F_k un sous-espace vectoriel N_{k+1} totalement isotrope, c'est-à-dire tel que $Tr_{F/K} x^2 = 0 \quad \forall x \in N_{k+1}$. Il vient également $Tr_{E/K} x^2 = 0 \quad \forall x \in N_{k+1}$ et N_{k+1} est totalement isotrope dans E.

Posons $M_{k+1} = M_k \perp N_{k+1}$. On a $\dim_K M_{k+1} = \dim_K M_k + \dim_K N_{k+1} = \frac{q^e - q^{e-k}}{2} + \frac{q^{e-k} - q^{e-k-1}}{2} =$
$= \frac{q^e - q^{e-k-1}}{2}$. Et $M_{k+1}^{\perp} = M_{k+1} \perp F_{k+1}$.

Nous obtenons finalement un sous-espace vectoriel $M_e = \overset{i=e}{\underset{i=1}{\perp}} N_i$ totalement isotrope et de dimension sur K égale à $\frac{q^e - 1}{2}$.

COROLLAIRE. - *Le sous-espace vectoriel* T *des éléments de trace nulle est un espace hyperbolique.*

Désignons par N_i' le sous-espace vectoriel engendré sur F_i par les vecteurs $\theta_i^j (j=h+1,\ldots,2h)$ et posons $T_i = N_i \oplus N_i'$.

Il vient : $E = (\overset{k=1}{\underset{k=1}{\perp}} T_k) \perp K1 = (M \oplus M') \perp K.1.$ avec $M = \overset{k=e}{\underset{k=1}{\perp}} N_k$ et $M' = \overset{k=e}{\underset{k=1}{\perp}} N_k'$.

Il en résulte que $T = M \oplus M'$; T est donc un espace hyperbolique de rang $q^e - 1$ sur K.

III - *EXTENSIONS NON RAMIFIEES.*

Dans cette partie, sauf mention du contraire, tous les anneaux considérés sont supposés être commutatifs et unitaires.

A. DEFINITIONS ET RAPPELS.

DEFINITION 3.1. - *Soient* R *un anneau (non nécessairement commutatif) et* M *un* R*-module. On dit que* M *est un* R*-module* générateur *s'il existe des éléments* $f_1,\dots,f_n$ *de* $\mathrm{Hom}_R(M,R)$ *et* $m_1,\dots,m_n$ *de* M *tels que* $\sum_{i=1}^{n} f_i(x_i)=1$.

On dit que M *est un* R*-module* progénérateur *si* M *est un* R*-module générateur et un* R*-module projectif de type fini.*

PROPOSITION 3.1. - *Soit* R *un anneau (non nécessairement commutatif). Pour un* R*-module* M*, les propositions suivantes sont équivalentes :*

a- Le R*-module* M *est projectif .*

b- Il existe une famille $(m_i)_{i\in I}$ *d'éléments de* M *et une famille* $(f_i)_{i\in I}$ *d'éléments de* $\mathrm{Hom}_R(M,R)$ *telle que :*

- $\forall m \in M$, $f_i(m)=0$ *sauf pour un nombre fini d'indices* $i\in I$,
- $\forall m \in M$, $\sum_{i\in I} f_i(m).m_i=m$.

La famille $(m_i,f_i)_{i\in I}$ est appelée *base duale* de M.

PROPOSITION 3.2. - *Si* R *est un anneau dont les seuls idempotents sont* 0 *et* 1, *alors tout* R-*module projectif de type fini (non réduit à* {0} *) est fidèle et progénérateur.*

COROLLAIRE. - *Si* R *est un anneau et* M *une* R-*algèbre telle que* M *soit un* R-*module progénérateur, alors* R *est facteur direct de toute sous-algèbre de* M *en tant que* R-*module.*

DEFINITION 3.2 (algèbre séparable). - *Soient* R *un anneau et* A *une* R-*algèbre. Nous désignons par* A° *l'algèbre opposée à* A *et par* A^e *la* R-*algèbre* $A \otimes_R A^\circ$, *dont la multiplication est définie par* $(a\otimes b).(a'\otimes b') = aa'\otimes b'b$. $\forall a,a',b' \in A$,

Nous pouvons munir A *d'une structure de* A^e-*module à gauche par l'opération* $(a\otimes b).x = axb$, $\forall a,x,b \in A$.

L'application $\mu : A^e \to A$ *définie par* $\mu(a\otimes b) = ab$ *est évidemment surjective et son noyau* J *est un idéal à gauche de* A^e *engendré par les éléments de la forme* $a \otimes 1 - 1 \otimes a$, $a \in A$.

On dit que la R-*algèbre* A *est* séparable *si elle vérifie l'une des propositions équivalentes suivantes :*

a- A *est une* A^e-*module projectif .*

b- La suite exacte de A^e-*modules à gauche* $0 \to J \to A^e \xrightarrow{\mu} A \to 0$ *est scindée.*

c- Il existe un élément e *de* A^e *tel que* $\mu(e)=1$ *et* $Je = \{0\}$ *(*e *est idempotent).*

Remarque .- Rappelons que, si R est un corps, une R-algèbre A est dite *séparable* au sens classique si le radical de Jacobson de $A \otimes_R K$ est nul pour toute extension K de R (N. BOURBAKI, *Algèbre*, Ch. 8).

On démontre qu'une R-algèbre A est séparable (lorsque R est un corps) si et seulement si elle est séparable au sens classique et si elle est un espace vectoriel de dimension finie sur R.

PROPOSITION 3.3. - *Si* A_1 *et* A_2 *sont deux* R*-algèbres séparables, la* R*-algèbre* $A_1 \otimes_R A_2$ *est alors séparable.*

Si A_1 *et* A_2 *sont deux* R*-algèbres telles que* $A_1 \otimes_R A_2$ *soit une* R*-algèbre séparable et* R *un facteur direct de* A_2 *en tant que* R*-module, alors* A_1 *est une* R*-algèbre séparable.*

PROPOSITION 3.4. - *Soient* S *une* R*-algèbre commutative et* A *une* R*-algèbre. Si* A *est une* R*-algèbre séparable, alors* $S \otimes_R A$ *est une* S*-algèbre séparable.*

PROPOSITION 3.5. - *Soit* A *une* R*-algèbre telle que* A *soit un* R*-module de type fini. Les assertions suivantes sont équivalentes :*

a- A *est une* R*-algèbre séparable .*

b- Pour tout idéal maximal $\mathfrak{m}$ *de* A, $A/\mathfrak{m}A$ *est une* $R/\mathfrak{m}$*-algèbre séparable.*

c- Pour tout idéal maximal $\mathfrak{m}$ *de* A, $A_{\mathfrak{m}}$ *est une* $R_{\mathfrak{m}}$*-algèbre séparable.*

PROPOSITION 3.6. - *Soient* A_1 *et* A_2 *deux* R-*algèbres. Les assertions suivantes sont équivalentes :*

a- $A_1 \times A_2$ *est une* R-*algèbre séparable.*

b- A_1 *et* A_2 *sont des* R-*algèbres séparables.*

(On peut trouver les démonstrations des résultats énoncés dans : F. DEMEYER et H. INGRAHAM , Separable Algebras Over Commutative Rings, *Lecture Notes in Mathematics* - Springer, Berlin (1971).

PROPOSITION 3.7. - *Soient* A *un anneau intègre et intégralement clos,* K *son corps des fractions,* K' *une* K-*algèbre séparable de dimension finie et* A' *la fermeture intégrale de* A *dans* K'. *Alors* A' *est contenu dans un* A-*module de type fini.*

Plus précisement, soit $(w_1,\ldots,w_n)$ une base de K' sur K contenue dans A' ; il y a alors une base unique $(w_1^*,\ldots,w_n^*)$ de K' sur K pour laquelle on a $\mathrm{Tr}_{K'/K}(w_i w_j^*) = \delta_{ij}$(indice de Kronecker) ; si d est le discriminant de la base $(w_1,\ldots,w_n)$, $d = D_{K'/K}(w_1,\ldots,w_n)$, on a $d \neq o$ et

$$\sum_{i=1}^{n} Aw_i \subset A' \subset \sum_{i=1}^{n} A\, w_i^* \subset d^{-1}\left(\sum_{i=1}^{n} A\, w_i\right) .$$

En particulier, si d est un élément inversible de A, A' est un A-module libre de base $(w_1,\ldots,w_n)$. (N. BOURBAKI, *Algèbre commutative*, Ch. V, § 1, Prop. 18).

COROLLAIRE.1. - *Si* A *est un anneau noethérien, le* A*-module* A' *est de type fini et en particulier* A' *est un anneau noethérien.*

COROLLAIRE 2. - *Si* A *est un anneau principal,* A' *est un* A*-module libre de rang* n.

DEFINITION 3.3 (Extension non ramifiée d'un anneau local). - *Soient* A *un anneau local, intègre et intégralement clos,* K *son corps des fractions et* $\mathfrak{m}$ *son idéal maximal. Soient* K' *une extension algébrique de degré* n *de* K, A' *un sous-anneau de* K' *contenant* A, *ayant* K' *pour corps des fractions et entier sur* A.

On dit que l'idéal maximal $\mathfrak{m}$ *de* A *est non ramifié dans* A', *s'il existe une base* $(w_1,\ldots,w_n)$ *de* K' *sur* K, *formée d'éléments de* A' *et dont le discriminant* $D_{K'/K}(w_1,\ldots,w_n)$ *appartient à* $A - \mathfrak{m}$.

Si $\mathfrak{m}$ est non ramifié dans A', K' est alors une extension séparable de K, A' est la fermeture intégrale de A dans K' et A' est un A-module libre de rang n dont toute base sur A est une base de K' sur K (N. BOURBAKI, *Algèbre commutative,* Ch. V, ex. 18).

DEFINITION 3.4 (Extension non ramifiée d'un anneau intègre . - *Soient* A *un anneau intègre et intègralement clos,* K *son corps des fractions,* K' *une extension algébrique de degré* n *de* K, A' *un sous-anneau de*

K' *contenant* A , *entier sur* A *et ayant* K' *pour corps des fractions.*

Si $\mathfrak{p}$ *est un idéal premier de* A, *on note* $A'_{\mathfrak{p}}$ *l'anneau des fractions de* A' *dont les dénominateurs sont dans* A - $\mathfrak{p}$

On dit que l'idéal premier $\mathfrak{p}$ *de* A *est* non ramifié *dans* A' *si l'idéal maximal* $\mathfrak{p}A_{\mathfrak{p}}$ *de* $A_{\mathfrak{p}}$ *est non ramifié dans* $A'_{\mathfrak{p}}$.

On dit que l'anneau A *est* non ramifié *dans* A' *(ou que* K' *est une extension* non ramifiée *de* K) *si tout idéal premier* $\mathfrak{p}$ *de* A *est non ramifié dans* A'.

PROPOSITION 3.8. - *Soient* A *un anneau intègre et intégralement clos,* K *son corps des fractions,* K' *une extension algébrique de degré* n *de* K *et* K" *une extension algébrique de degré* n' *de* K' . *On désigne par* A' *la fermeture intégrale de* A *dans* K' *et par* A" *la fermeture intégrale de* A' *dans* K".

Les assertions suivantes sont équivalentes :

a) A *est non ramifié dans* A",

b) A *est non ramifié dans* A' *et* A' *est non ramifié dans* A".

(N. BOURBAKI, *Algèbre commutative,* Ch. V, ex. 19).

DEFINITION 3.5. (Indice de ramification et degré résiduel). - *Soient* A *un anneau de Dedekind,* K *son corps des fractions,* K' *une extension algébrique séparable de degré* n *de* K *et* A' *la fermeture intégrale*

de A *dans* K'. *Pour tout idéal premier* $\mathfrak{p}$ *de* A, *les idéaux premiers de* A' *figurant dans la décomposition de* $\mathfrak{p}$ A' *sont exactement les idéaux premiers* $\mathfrak{P}$ *de* A' *situés au-dessus de* $\mathfrak{p}$; *On notera* $e_{\mathfrak{P}}$ *l'exposant de* $\mathfrak{P}$ *dans la décomposition en idéaux premiers de* $\mathfrak{p}$A' : $\mathfrak{p}A' = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}}$.

L'entier $e_{\mathfrak{p}}$ *est appelé l'* indice de ramification *de* $\mathfrak{p}$ *dans l'extension* K' *de* K. *D'autre part, comme* A' *est un* A-*module de type fini* (prop. 3.6. cor. 1), *alors pour tout idéal premier* $\mathfrak{P}$ *de* A' *situé au-dessus de* $\mathfrak{p}$, $A'/\mathfrak{P}$ *est une extension de degré fini de* $A/\mathfrak{p}$. *Le degré de cette extension est noté* $f_{\mathfrak{P}}$ *et est appelé le* degré résiduel *de* $\mathfrak{p}$ *dans l'extension* K' *de* K.

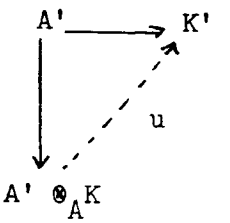
De plus, l'anneau $A'/\mathfrak{p}A'$ *est une* $A/\mathfrak{p}$*-algèbre de degré* n, *isomorphe au produit* $\prod_{\mathfrak{P}|\mathfrak{p}} A'/\mathfrak{P}$ *et on a la formule :* $n = \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}}$

(J.P. SERRE, *Corps Locaux*, Ch. 1, § 4).

B - CARACTERISATION DES EXTENSIONS NON RAMIFIEES.

LEMME 1. - *Soient* A *un anneau intègre et intégralement clos,* K *son corps des fractions,* K' *une extension algébrique de degré* n *de* K, A' *un sous-anneau de* K' *contenant* A, *entier sur* A *et ayant* K' *pour corps des fractions. On suppose que* A' *est un* A-*module de type fini. Alors* $A' \otimes_A K = K'$.

L'application A-linéaire $A' \to K$ se prolonge en une application K-linéaire unique $u : A' \otimes_A K \to K'$ telle que $u(x \otimes 1) = x$, $\forall x \in A'$.



Soit $y \in A' \otimes_A K$; posons $y = \alpha^{-1}(x \otimes 1)$ avec $\alpha \in A$, $\alpha \neq 0$, $x \in A'$. Si $u(y) = o$, on a $\alpha^{-1}.x = o$ dans K'; donc $x = o$ et $y = o$. L'application u est donc injective et est un homomorphisme de K-algèbres. La K-algèbre $A' \otimes_A K$ est alors de rang fini et intègre ; c'est donc un corps (N. BOURBAKI, *Algèbre*, Ch. V, § 2, n° 1). Comme K' est le corps des fractions de A', il s'ensuit que $A' \otimes_A K = K'$.

PROPOSITION 3.9. - *Soient* A *un anneau local intègre et intégralement clos, d'idéal maximal* $\mathfrak{m}$ *, de son corps des fractions,* K' *une extension algébrique de degré* n *de* K *et* A' *la fermeture intégrale de* A *dans* K'.

Les propositions suivantes sont équivalentes :

a- $\mathfrak{m}$ *est non ramifié dans* A'

b- A' *est une* A*-algèbre séparable, de type fini en tant que* A*-module.*

a $\Rightarrow$ b . Il existe une base $(w_1,\ldots,w_n)$ de K' sur K formée d'éléments de A' et telle que le discriminant $D_{K'/K}(w_1,\ldots,w_n)$ appartienne à $A-\mathfrak{m}$. La A-algèbre A' est alors libre et admet pour base $(w_1,\ldots,w_n)$ (prop. 3.7) et $A'/\mathfrak{m}A'$ est une $A/\mathfrak{m}$-algèbre libre dont la base $(w_1,\ldots,w_n)$ est telle que $D_{A'/\mathfrak{m}A'\,/\,A/\mathfrak{m}}(\bar{w}_1,\ldots,\bar{w}_n) \neq 0$. Donc $A'/\mathfrak{m}A'$ est une $A/\mathfrak{m}$-algèbre séparable et par suite A' est une A-algèbre séparable (prop. 3.5).

D'après le lemme précédent, K' s'identifie à $A' \otimes_A K$ et, par suite, est une K-extension séparable (prop. 3.4). D'autre part, A' étant une A-algèbre séparable, il existe un idempotent $e = \sum_{j=1}^{m} x_j \otimes y_j$ de $A' \otimes_A A'$ tel que :

$\sum_{j=1}^{m} x_j y_j = 1$ et $(1 \otimes x - x \otimes 1)e = o \quad \forall x \in A'$.

Soit Ω une clôture algébrique de K. Pour un K-isomorphisme σ de K' dans Ω nous désignerons par σ' sa restriction à A'. Nous savons qu'il y a exactement n K-isomorphismes $\sigma_1, \ldots, \sigma_n$ de K' dans Ω et, pour $i \neq j$, on a $\sigma_i' \neq \sigma_j'$; en effet, soit $y \in K'$ et posons $y = xz^{-1}$, $x \in A'$, $z \in A'$, $z \neq o$, on a $\sigma_i(y) = \sigma_i(x)(\sigma_i(z))^{-1} = \sigma_i'(x)(\sigma_i'(z))^{-1}$; il en résulte que $\sigma_i' = \sigma_j'$ entraîne $\sigma_i = \sigma_j$.

La restriction σ' d'un K-isomorphisme σ de K' à A' est un isomorphisme de A' sur $\sigma'(A')$ par suite $1_{A'} \otimes \sigma' : A' \otimes_A A' \to A' \otimes_A \sigma'(A')$ est un isomorphisme. Désignons par $\mu : A' \otimes_A \sigma'(A') \to A'\sigma'(A')$ l'application définie par $\mu(\sum_i a_i \otimes \sigma'(a_i')) = \sum_i a_i \sigma(a_i')$; μ est un homomorphisme d'algèbres. Posons $e_\sigma = \mu[(1_A \circ \sigma')(e)]$; e_σ est évidemment un idempotent de $A'\sigma'(A)$.

Soit x un élément de A, nous avons :

$$xe_\sigma = x.[\mu(1_{A'} \otimes \sigma')(e)] = \mu[(x \otimes 1)(1_{A'} \otimes \sigma)(e)] = \mu[(1_{A'} \otimes \sigma)((x \otimes 1).e)]$$

$$= \mu[(1_{A'} \otimes \sigma')((1 \otimes x).e)] = \mu[(1_{A'} \otimes \sigma).(1 \otimes x)]e_\sigma = \sigma'(x)e_\sigma.$$

Ainsi, $(x - \sigma'(x))e_\sigma = 0, \quad \forall x \in A'$.

Si $e_\sigma = o$, on a $x = \sigma'(x)$, $\forall x \in A'$, d'où $\sigma' = 1_{A'}$; donc $\sigma = 1_{K'}$ et

$$e_\sigma = \sum_{j=1}^{\mathfrak{m}} x_j \sigma'(y_j) = \sum_{j=1}^{\mathfrak{m}} x_j y_j = 1.$$

Donc, pour un K-isomorphisme σ de K', on a $e_\sigma = \delta_{\sigma, 1_{K'}}$. Il en résulte que pour tout élément x de A', nous avons :

$$\sum_{j=1}^{m} x_j \mathrm{Tr}(y_j x) = \sum_{j=1}^{m} x_j \Big(\sum_{k=1}^{n} \sigma_k(y_j x) \Big) = \sum_{j=1}^{m} x_j \Big(\sum_{k=1}^{n} \sigma_k(y_j)\sigma_k(x) \Big)$$

$$= \sum_{k=1}^{n} \sigma_k(x) \Big(\sum_{j=1}^{m} x_j \sigma_k(y_j) \Big) = \sum_{k=1}^{n} \sigma_k(x) e_{\sigma_k} = x \quad .$$

Cela entraine que A' est une A-algèbre libre (prop. 3.1) et que $A'/\mathfrak{m}A'$ est une $A/\mathfrak{m}$-algèbre séparable (prop. 3.5) de rang n.

Soit $(w_1, \ldots, w_n)$ une base de A' sur A, les images $(\bar{w}_1, \ldots, \bar{w}_n)$ forment évidemment une base de $A'/\mathfrak{m}A'$ sur $A/\mathfrak{m}$, dont le discriminant $D_{A'/\mathfrak{m}A'/(A/\mathfrak{m})}(\bar{w}_1, \ldots, \bar{w}_n)$ est non nul ; par suite, le discriminant $D_{K'/K}(w_1, \ldots, w_n)$ est un élément de $A - \mathfrak{m}$ et $\mathfrak{m}$ est non ramifié dans A'.

REMARQUE. - L'une ou l'autre des propositions a et b du résultat précédent entraine la proposition suivante :

La forme A-bilinéaire B sur A' définie par $(x,y) \mapsto \mathrm{Tr}_{K'/K}(xy)$ *est non dégénérée.*

Si $\mathfrak{M}$ est non ramifié dans A', il existe une base $(w_1,\ldots,w_n)$ de K' sur K, qui est aussi une base de A' sur A, et dont le discriminant $D_{K'/K}(w_1,\ldots,w_n) = \det\left[\mathrm{Tr}_{K'/K}(w_i w_j)\right]$ est inversible dans A. La forme A-bilinéaire B est alors non dégénérée.

THEOREME 3.1. - *Soient* A *un anneau de Dedekind,* , K *son corps des fractions,* K' *une extension algébrique de degré* n *sur* K, *séparable sur* K *et* A' *la fermeture intégrale de* A *dans* K'. *Les propositions suivantes sont équivalentes :*

a- L'anneau A *est non ramifié dans* A',

b- A' *est une* A*-algèbre séparable.*

c- La forme A*-bilinéaire* B *définie sur* A' *par* $(x,y) \mapsto \mathrm{Tr}_{K'/K}(xy)$ *est non dégénérée.*

d- Pour tout didéal premier $\mathfrak{p}$ *de* A, *l'indice de ramification* $e_{\mathfrak{P}}$ *de tout idéal premier* $\mathfrak{P}$ *de* A' *situé au-dessus de* $\mathfrak{p}$ *est égal à 1 et* $A'/\mathfrak{P}$ *est une* $A/\mathfrak{P}$ *-algèbre séparable.*

- Cas local.

Supposons que A soit un anneau de valuation discrète d'idéal maximal $\mathfrak{M}$. Nous asavons que dans ces conditions A' est un A-module libre de rang n (prop. 3.7., cor. 2).

Les propositions a et b sont évidemment équivalentes et l'une quelconque d'entre elles entraine la proposition c (remarque précédente).

c $\Rightarrow$ a . Si B est non dégénérée, toute base du A-module A' a son discriminant dinversible dans A ; or toute base du A-module A' est une base de K' sur K car $A' \otimes_A K = K'$ (lemme 1).

a $\Leftrightarrow$ d . Si $\mathfrak{m}$ est non ramifié dans A', A' est une A-algèbre séparable et par suite $A'/\mathfrak{m}A'$ est une $A/\mathfrak{m}$-algèbre séparable (prop. 3.5).
Comme $A'/\mathfrak{m}A'$ est sans radical et $\mathfrak{m}A'$ est contenu dans le radical de A', on a $\mathfrak{m}A' = \mathrm{Rad}(A')$. Désignons par $\mathfrak{m}'_1,\ldots,,\mathfrak{m}'_r$ les idéaux maximaux de A' ; on a $\mathfrak{m}A' = \bigcap_{i=1}^{i=r} \mathfrak{m}'_i = \prod_{i=1}^{i=r} \mathfrak{m}'_i$ et $A'/\mathfrak{m}A'$ est isomorphe à $\prod_{i=1}^{r} A'/\mathfrak{m}'_i$ en tant que $A/\mathfrak{m}$-algèbre. Pour tout indice $i=1,\ldots,r$ l'indice de ramification e_i de $\mathfrak{m}'_i$ est égal à 1 et $A'/\mathfrak{m}'_i$ est une $A/\mathfrak{m}$-algèbre séparable (prop. 3.6).
Réciproquement, si la proposition d est vérifiée, $\mathfrak{m}A'$ est évidemment le radical de A' et $A'/\mathfrak{m}A'$ est isomorphe à $\prod_{i=1}^{r} A'/\mathfrak{m}'_i$ en tant que $A/\mathfrak{m}$-algèbre ($\mathfrak{m}'_1,\ldots,\mathfrak{m}'_r$ étant les idéaux maximaux de A'). Comme chacune des $A/\mathfrak{m}$-algèbres $A'/\mathfrak{m}'_i$ est séparable, leur produit l'est aussi (prop. 3.6) et par suite $A'/\mathfrak{m}A'$ est alors une $A/\mathfrak{m}$-algèbre séparable. Il en résulte que A' est une A-algèbre séparable (prop. 3.5).

- Cas d'un anneau de Dedekind.

Nous supposons maintenant que A est un anneau de Dedekind.
Pour tout idéal premier $\mathfrak{p}$ de A; $A_{\mathfrak{p}}$ est un anneau de valuation discrète dont K est le corps des fractions et $A'_{\mathfrak{p}}$ est la fermeture intégrale de $A_{\mathfrak{p}}$ dans K'.

Nous désignerons par $\mathfrak{P}_1,\ldots,\mathfrak{P}_r$ les idéaux premiers de A' situés au dessus de l'idéal premier $\mathfrak{p}$ de A et par $e_1,\ldots,e_r$ leurs indices de ramification reppectifs : $\mathfrak{p}A' = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$.

Nous savons que A' est un A-module de type fini (prop. 3.7, cor.1) et que $A'_{\mathfrak{p}}$ est un $A_{\mathfrak{p}}$ -module libre de rang n (prop. 3.7, cor. 2). D'autre part, les e_i sont aussi les indices de ramification des idéaux premiers de $A'_{\mathfrak{p}}$ situés au-dessus de $\mathfrak{p}A_{\mathfrak{p}}$.

Enfin, considérons la forme bilinéaire B' définie sur le $A_{\mathfrak{p}}$-module $A'_{\mathfrak{p}}$ par $(x,y) \mapsto \mathrm{Tr}_{K'/K}(xy)$; il est clair que $B' = B_{\mathfrak{p}}$, car les modules $(A'^{*})_{\mathfrak{p}}$ et $(A'_{\mathfrak{p}})^{*}$ sont isomorphes.

a $\Leftrightarrow$ b . Si A est non ramifié dans A', alors pour tout idéal premier $\mathfrak{p}$ de A, $A'_{\mathfrak{p}}$ est une $A_{\mathfrak{p}}$-algèbre séparable (prop. 3.9) et par suite A' est une A-algèbre séparable (prop. 3.5) (dans un anneau de Dedekind, tout idéal premier non nul est maximal). Réciproquement, si A' est une A-algèbre séparable, alors pour tout idéal premier $\mathfrak{p}$ non nul de A, $A'_{\mathfrak{p}}$ est une $A_{\mathfrak{p}}$-algèbre séparable. Donc tout idéal premier non nul est non ramifié dans A'. L'idéal $\{o\}$ est non ramifié dans A' car K' est une extension séparable de K. L'anneau A est par suite non ramifié dans A'.

a $\Leftrightarrow$ c . Si A est non ramifié dans A', alors pour tout idéal premier $\mathfrak{p}$ de A, l'idéal $\mathfrak{p}A_{\mathfrak{P}}$ est non ramifié dans A' et la forme $A_{\mathfrak{p}}$ -bilinéaire $B_{\mathfrak{p}}$ est non dégénérée. Comme toutes les formes localisées $B_{\mathfrak{p}}$ sont non dégénérées, la forme B l'est aussi.

Inversement, si B est non dégénérée, alors pour tout idéal premier non nul $\mathfrak{p}$ de A, $B_{\mathfrak{p}}$ est non dégénérée. Par suite, tout idéal premier non nul de A est non ramifié dans A'. Comme l'idéal premier $\{0\}$ de A est évidemment non ramifié dans A', l'anneau A alors non ramifié dans A'.

a $\Leftrightarrow$ d. Si A est non ramifié dans A', alors pour tout idéal premier $\mathfrak{p}$ de A, les indices de ramification des idéaux premiers de $A'_{\mathfrak{p}}$ situés au-dessus de $\mathfrak{p}A_{\mathfrak{p}}$ sont égaux à 1. Donc, pour tout idéal premier $\mathfrak{p}$ de A. les indices de ramifications $e_1,\ldots,e_r$ des idéaux premiers $\mathfrak{P}_1,\ldots,\mathfrak{P}_r$ de A' situés au dessus de $\mathfrak{p}$ sont tous égaux à 1. D'autre part, comme A' est une A-algèbre séparable, $A'/\mathfrak{p}A'$ est aussi une $A/\mathfrak{p}$ -algèbre séparable (prop. 3.5) ; or $A'/\mathfrak{p}A'$ est isomorphe à $\prod_{i=1}^{r} A'/\mathfrak{p}_i$ en tant que $A/\mathfrak{p}$ -algèbre ; il en résulte que chacune des $A/\mathfrak{p}$ -algèbres $A'/\mathfrak{p}_i$ est séparable (prop. 3.6).

Inversement, si la proposition d est satisfaite, $A'/\mathfrak{p}A'$ est isomorphe à la $A/\mathfrak{p}$ -algèbre $\prod_{i=1}^{r} A'/\mathfrak{p}_i$; $A'/\mathfrak{p}A'$ est donc une $A/\mathfrak{p}$ -algèbre séparable (prop. 3.6) pour tout idéal premier $\mathfrak{p}$ de A. Par suite, A' est une A-algèbre séparable et A est non ramifié dans A'.

COROLLAIRE. - *On désigne par* T *le sous-*A*-module des éléments de trace nulle de* A' : T *n'est autre que l'orthogonal de* $A.\,1_{A'}$ *dans le* A*-module bilinéaire* (A',B). *On suppose l'entier* n *inversible dans* A. *Alors* $A' = A \perp T$ *et les propositions suivantes sont équivalentes :*

a- A *est non ramifié dans* A' ·

b- *Le* A-*module bilinéaire* (T,B/T×T) *est non dégénéré.*

L'hypothèse "n inversible dans A" entraine que le sous A-module de A' est fortement non isotrope , d'où la décomposition de A' sous la forme A' = $A \perp A^{\perp} = A \perp T$ (prop. 1.2).

a $\Rightarrow$ b . La forme A-bilinéaire B étant non dégénérée et le facteur direct $A.1_{A'}$ étant fortement non isotrope, le facteur direct T est alors fortement non isotrope, c'est-à-dire que le A-module (T, B/T×T) est non dégénéré.

b $\Rightarrow$ a · Le A-module bilinéaire (A,B) est non dégénéré, car il est la somme directe orthogonale de deux A-modules bilinéaires non dégénérés ;

par conséquent, A est non ramifié dans A'.

C - PROPRIETES DES EXTENSIONS NON RAMIFIEES.

THEOREME 3.2. - *Soient* A *un anneau de Dedekind,* K *son corps des fractions,* K' *une extension algébrique séparable de degré* n *de* K. *On suppose de plus que* K' *est le produit tensoriel de* q *extensions algébriques séparables* K_i *de degré* n_i *de* K. *On désigne par* A' *la fermeture intégrale de* A *dans* K *et par* A'_i *la fermeture intégrale de* A *dans* K_i. *Les propositions suivantes sont équivalentes :*

a- *Pour tout* i, A *est non ramifié dans* A'_i.

b- $A' = \bigotimes_{i=1}^{i=q} A'_i$ *et* A *est non ramifié dans* A'.

a $\Rightarrow$b .

- Cas local. On suppose que A est un anneau de valuation discrète, d'idéal maximal $\mathfrak{m}$.

La démonstration se fait par récurrence sur l'entier q.

La proposition est évidente pour q=1. Supposons-la vraie jusqu'à l'ordre q-1 et posons : $K' = \bigotimes_{i=1}^{q} K_i = \left(\bigotimes_{i=1}^{q-1} K_i\right) \otimes_K K_q = F \otimes_K K_q$ avec $f = \bigotimes_{i=1}^{q-1} K_i$, $\dim_K F = n_1 \ldots n_{q-1}$. Désignons par B la fermeture intégrale de A dans F. $\mathfrak{m}$ est non ramifié dans B et $B = \bigotimes_{i=1}^{q-1} A'_i$. Comme B et A'q sont entiers sur A, leur produit tensoriel $B \otimes_A A'q$ l'est aussi (N. BOURBAKI, *Algèbre*, Ch. V, § 1, n° 1) et $B \otimes_A A'q \subset A'$. Il existe une base $(e_i)_{1 \leq i \leq n_1, \ldots, n_{q-1}}$ de F contenue dans B et une base $(f_j)_{1 \leq j \leq n_q}$ de K_q sur K contenue dans A'_q, dont les discriminants respectifs sont inversibles dans A; La famille

$(e_i \otimes f_j)_{\substack{1 \leq i \leq n_1 \ldots n_{q-1} \\ 1 \leq j \leq n_q}}$ est une base de K' sur K contenue dans A'.

Calculons le discriminant de cette base ; à cet effet, considérons les applications linéaires suivantes :

ϕ_1 est l'application linéaire de F dans K définie par : $x_1 \mapsto \mathrm{Tr}_{F/K}(x_1)$,

ϕ_2 est l'application linéaire de K_q dans K définie par $x_2 \mapsto \mathrm{Tr}_{K_q/K}(x_2)$.

Le produit tensoriel $\phi_1 \otimes \phi_2$ est défini par

$$(\phi_1 \otimes \phi_2)(x_1 \otimes x_2) = \phi_1(x_1).\phi_2(x_2) = \mathrm{Tr}_{F/K}(x_1).\mathrm{Tr}_{K_q/K}(x_2) = \mathrm{Tr}_{F \otimes K_q/K}(x_1 \otimes x_2).$$

Le discriminant D de la base $(e_i \otimes f_j)_{\substack{1 \leq i \leq n_1 \ldots n_{q-1} \\ 1 \leq j \leq n_q}}$ est donné par $D = (\det \phi_2)^{n_1 \ldots n_{q-1}} . (\det(\phi_1))^{n_q}$. Le scalaire D est un élément inversible de A; donc $\mathfrak{m}$ est non ramifié dans $B \otimes_A A'_q$. Il en résulte que $A' = B \otimes_A A'_q = \bigotimes_{i=1}^{q} A'_i$ (déf. 3.3).

- Cas d'un anneau de Dedekind. On suppose maintenant que A est un anneau de Dedekind. Comme A est non ramifié dans A'_i, alors pour tout idéal premier $\mathfrak{p}$ de A, l'idéal maximal $\mathfrak{p} A_{\mathfrak{p}}$ de $A_{\mathfrak{p}}$ est non ramifié dans $(A'_i)_{\mathfrak{p}}$, fermeture intégrale de $A_{\mathfrak{p}}$ dans K_i. Il en résulte que l'idéal maximal $\mathfrak{p} A_{\mathfrak{p}}$ est non ramifié dans $A'_{\mathfrak{p}}$, pour tout idéal premier $\mathfrak{p}$ de A. Par suite, A est non ramifié dans A'.

Il nous reste à montrer que $A' = \bigotimes_{i=1}^{q-1} A'_i$. Posons encore $B = \bigotimes_{i=1}^{q-1} A'_i$; il est clair que $B \subset A'$. D'autre part, $(\bigotimes_{i=1}^{q} A'_i)_{\mathfrak{p}} = \bigotimes_{i=1}^{q} (A'_i)_{\mathfrak{p}}$; or ce dernier anneau est intégralement clos dans son corps des fractions ; donc B est intégralement clos dans son corps des fractions. Par suite, $B \supset A'$ et finalement $B = A'$.

b $\Rightarrow$ a .

- Cas local. Supposons que A soit un anneau de valuation discrète d'idéal maximal $\mathfrak{m}$. Pour tout indice i=1,...q, A'_i est un A-module libre de rang fini (prop. 3.7, cor. 2). Par suite, A est facteur direct de chaque A'_i en tant que A-module (prop. 3.2, corollaire). Comme A est non ramifié

dans A', A' est une A-algèbre séparable (théorème 3.1) ; donc pour chaque indice i, A'_i est une A-algèbre séparable (prop. 3.3). L'anneau A est alors non ramifié dans chaque A'_i.

- Cas d'un anneau de Dedekind. On suppose maintenant que A est un anneau de Dedekind. Pour tout idéal premier $\wp$ de A, l'anneau de valuation discrète $A_\wp$ est non ramifié dans $A'_\wp$; or $A'_\wp = (\bigotimes_{i=1}^{q} A'_i)_p = \bigotimes_{i=1}^{q} (A'_i)_p$; donc pour tout idéal premier $\wp$ de A, l'idéal maximal $\wp A_\wp$ est non ramifié dans chacun des $(A'_i)_\wp$. Par conséquent A est non ramifié dans chacun des A'_i.

THEOREME 3.3. - *Soient* A *un anneau de Dedekind,* K *son corps des fractions,* K' *une extension non ramifiée de degré* n *de* K *et* A' *la fermeture intégrale de* A *dans* K'. *On désigne par* T *le sous-*A*-module des éléments de trace nulle de* A'.

Nous avons les propriétés suivantes :

a- La suite de A*-modules* $0 \to T \to A' \xrightarrow{Tr} A \to 0$ *est exacte et scindée.*

b- Le A*-module* T *est projectif de rang* n-1 .

c- Si A' *est un* A*-module libre, alors* T *est un* A*-module libre de rang* n-1.

Le A-module A' est projectif de rang n ; c'est donc un A-module générateur (prop. 3.2). Par suite, il existe des éléments $f_1,\ldots,f_n$ de $\mathrm{Hom}_A(A',A)$ et des éléments $x_1,\ldots,x_n$ de A' tels que $\sum_{i=1}^{n} f_i(x_i)=1$. La forme A-bilinéaire B définie sur A' par $(x,y)\mapsto \mathrm{Tr}_{K'/K}(xy)$ étant non dégénérée (Théorème 3.1), il existe pour chaque indice $i=1,\ldots,n$ un élément $y_i \in A'$ tel que $f_i(x_i) = \mathrm{Tr}_{K'/K}(x_iy_i)$. Posons $c = \sum_{i=1}^{c} x_iy_i$; nous avons $\mathrm{Tr}_{K'/K}(c)=\mathrm{Tr}_{K'/K}(\sum_{i=1}^{n} x_iy_i) = \sum_{i=1}^{n} \mathrm{Tr}_{K'/K}(x_iy_i) = \sum_{i=1}^{n} f_i(x_i)=1$, ce qui démontre l'assertion a .

Il en résulte que T est un facteur direct du A-module projectif A' de rang n ; C'est donc un A-module projectif de rang n-1 ; d'où b .

Comme la suite $0 \to T \to A' \xrightarrow{\mathrm{Tr}} A \to 0$ est exacte, nous avons $C(A') = C(T)+ C(A)$. Si A' est un A-module libre, alors $C(A')=C(A)=0$ (Théorème 1.3, lemme 1); d'où $C(T) = o$. Le A-module T est, dans ce cas, libre de rang n-1 (Théorème 1.3, lemme 1).

COROLLAIRE. - *Sous les hypothèses de la proposition précédente, il existe au moins un élément* x *de* A *tel que* $\mathrm{Tr}_{K'/K}(x) = 1$.

D - CARACTERISATION DES EXTENSIONS CYCLIQUES DU TYPE D'ARTIN-SCHREIER NON RAMIFIEES.

Soient A un anneau de Dedekind, K son corps des fractions, K' une extension algébrique séparable de degré n de K et A' la fermeture intégrale de A dans K' .

THEOREME 3.4. - *Si* K' *est une extension cyclique A.S.S., les propositions suivantes sont équivalentes :*

a- A *est non ramifié dans* A'.

b- L'extension K' *de* K *est engendrée par une racine d'un polynôme irréductible de* $K[X]$ *de la forme* $X^p - X - a$, *où* $a \in A$.

b $\Rightarrow$ a . Soit θ une racine du polynôme irréductible $X^p - X - a$. L'extension $K' = K(\theta)$ est une extension cyclique de degré p de K et les autres racines du polynômes $X^p - X - a$ sont $\theta+1, \theta+2, \ldots, \theta+p-1$. Par suite, le discriminant de la base $(1, \theta, \ldots, \theta^{p-1})$ de K' sur K est

$D_{K'/K}(1, \theta, \ldots, \theta^{p-1}) = \det[Tr_{K'/K}(\theta^i \theta^j)] = (-1)^{\frac{p-1}{2}}$. La valeur de ce discriminant étant un élément inversible de A, A' est alors un A-module libre de rang p admettant pour base $(1, \theta, \ldots, \theta^{p-1})$ (Prop. 3.7) et la forme A-bilinéaire B définie sur A' par $(x,y) \mapsto Tr_{K'/K}(xy)$ est non dégénérée ; A est alors non ramifié dans A'.

a $\Rightarrow$ b . Il existe un élément v de A' tel que $Tr_{K'/K}(v)=1$ (théorème 3.3, corollaire). Comme $v \notin K$, il vient $K' = K(v)$. Désignons par σ un générateur du groupe de Galois de K' sur K. Nous avons $\alpha-\sigma(\alpha) = 1$ avec $\alpha = v+2\sigma(v)+\ldots+(p-1)\,\sigma^{(p-2)}(v)$; d'où $\sigma(\alpha^p-\alpha)=[\sigma(\alpha)]^p-\sigma(\alpha)=(\alpha-1)^p-\alpha^p-1=\alpha^p-\alpha$, avec $a=\alpha^p-\alpha \in A$ et par suite α est racine du polynôme $X^p-X-a \in K[X]$.

THEOREME 3.5. - *Soit* K' *une extension cyclique A.S.G. de* K. *On désigne par* $F_1,\ldots,F_{e-1}$ *les corps intermédiaires entre* K *et* K' *de degrés sur* K *respectivement égaux à* $p^{e-1},\ldots,p$ *et par* A'_i *la fermeture intégrale de* A *dans* F_i $(i=1,\ldots,e-1)$. *On pose* $A=A'_e$, $A'=A'_o$, $K=F_e$ *et* $K'=F'_o$. *Les assertions suivantes sont équivalentes :*

a- A *est non ramifié dans* A' .

b- Pour tout indice $i=o,1,\ldots,e-1$, F_i *est une extension cyclique de degré* p *de* F_{i+1} *engendrée par une racine d'un polynôme irréductible de la forme* X^p-X-a_{i+1} *de* $F_{i+1}[X]$ *où* $a_{i+1} \in A_{i+1}$.

a $\Rightarrow$ b . Si A est non ramifié dans A', alors, pour tout indice $i=o,1,\ldots,e-1$, A_{i+1} est non ramifié dans A_i (prop. 3.8) et l'assertion b découle immédiatement du théorème précédent.

b $\Rightarrow$ a . Pour tout indice $i=o,1,\ldots,e-1$, A_{i+1} est non ramifié dans A_i et A est alors non ramifié dans A' (prop. 3.8).

REMARQUE. - Il existe des extension du type d'Artin-Schreier qui se ramifient . Soient K' une extension cyclique A.S.S. de K ; K' est engendrée par

une racine d'un polynôme irréductible $X^p-X-a \in K[X]$ avec $a \in K$. Nous allons montrer qu'il n'est pas toujours possible de trouver un polynôme de la forme X^p-X-b, $b \in A$, tel que K' soit engendré par une racine de ce polynôme. Nous rappelons que le corps des racines sur K des polynômes X^p-X-a et X^p-X-b coïncident si et seulement s'il existe $k \in \mathbb{Z}$, $1 \leq k \leq p-1$, et $c \in K$ tels que $b=ka+c^p-c$.

Soit $A = \mathbb{F}_p[X]$ l'anneau des polynômes à une variable sur le corps premier à p éléments $\mathbb{F}_p$; A est un anneau principal de caractéristique p dont le corps des fractions est $K = \mathbb{F}_p(X)$. Considérons le polynôme Y^p-Y-1/X de $K[Y]$. Ce polynôme est irréductible dans $K[Y]$, sinon il admettrait une racine dans K de la forme P/Q , où P et Q sont des polynômes de A premiers entre eux et nous aurions : $\frac{P^p}{Q^p} - \frac{P}{Q} - \frac{1}{X} = 0 \Rightarrow XP(P^{p-1}-Q^{p-1})=0$; alors P diviserait Q, ce qui est impossible.

Supposons qu'il existe un polynôme de la forme Y^p-Y-a, $a \in A$, tel que K' soit engendré par une de ces racines. Alors, il existe $k \in \mathbb{Z}$, $1 \leq k \leq p-1$, et deux polynômes P et Q de A premiers entre eux, tels que $k/X + \frac{P^p}{Q^p} - \frac{P}{Q} = a \in A$.

Il s'ensuit que $\frac{kQ^p+XP(P^{p-1}-Q^{p-1})}{XQ^p} \in A$, c'est-à-dire que X divise Q. En posant Q = XR, alors $\frac{R^{p-1}X^{p-1}(kR-P)+P^p}{X^p R^p} \in A$ et, par suite, P et Q ne sont pas premiers entre eux, ce qui est contradictoire.

IV - *ELEMENTS DE TRACE NULLE DANS UNE EXTENSION CYCLIQUE NON RAMIFIEE.*

Nous nous placerons dans la situation suivante :

A est un anneau de Dedekind de caractéristique p, dont on désigne par K le corps des fractions ; K' est une extension algébrique séparable de degré n de K et A' est la fermeture intégrale de A dans K'. Nous notons T le sous-A-module des éléments de trace nulle de A' et B la forme bilinéaire définie sur le A-module A' par $(x,y) \mapsto \mathrm{Tr}_{K'/K}(xy)$.

A - CAS DES EXTENSIONS CYCLIQUES DU TYPE D'ARTIN-SCHREIER.

THEOREM 4.1. - *Si* K' *est une extension cyclique non ramifiée A.S.S. ou A.S.G., nous avons les propriétés suivantes :*

a- le A*-module* A' *est libre de rang* n ; *de plus si* p *est différent de 2,* A' *admet une base orthogonale ;*

b- le A*-module* T *est libre de rang* n-1.

De plus, si K' *est une extension cyclique du type d'Artin-Schreier simple,* A' *est alors un* A*-module libre de rang* n *de la forme* $A'=A[\theta]$.

C'est une conséquence immédiate des théorèmes 3.4, 3.5, 3.6 et de la remarque suivant la proposition 2.4.

B - CAS DES EXTENSIONS CYCLIQUES DU TYPE DE KUMMER.

a) Extensions cycliques du type de Kummer de degré impair.

On suppose 2 et n inversibles dans l'anneau A.

THEOREME 4.2. - *Si* K' *est une extension cyclique non ramifiée* K.S. *ou* K.G. , *de degré impair sur* K, *alors :*

a- le A*-module bilinéaire* T *est un espace hyperbolique du type fini ;*

b- tout élément de T *s'écrit d'une manière unique sous la forme* $x=y+z$, *avec* $Tr_{K'/K}(y^2)= Tr_{K'/K}(z^2) = o$.

L'entier n étant inversible dans A, le A-module A se décompose sous la forme $A' = A\,1_{A'} \perp T$. Les modules bilinéaires (A',B) et (T,B/T × T) sont non dégénérés puisque K' est une extension non ramifiée de K (Théorème 3.1., corollaire). Désignons par W le sous-espace vectoriel des éléments de trace nulle de K' ; W est un espace hyperbolique de rang n-1 (prop. 2.7, corollaire) et nous avons évidemment $T = W \cap A$. D'autre part, comme $K' = K \otimes_A A'$, la forme bilinéaire non dégénérée B a même indice que la forme bilinéaire non dégénérée définie sur K' par $(x,y) \mapsto Tr_{K'/K}(xy)$ (prop. 1.3). Il en résulte que T est un espace hyperbolique de type fini.

COROLLAIRE. - *Les* A*-modules* A *et* T *sont libres de rang* n *et* n-1.

Comme T est un espace hyperbolique de tyep fini sur l'anneau de Dedekind A, c'est un A-module libre de rang n-1 ; par suite $A' = A.1_{A'} \perp T$ est un A-module libre de rang n.

THEOREME 4.3. - *On se place dans les hypothèses suivantes :*

- $n = q_1^{e_1} \dots q_1^{e_1}$, *où* $q_1,\dots,q_s$ *sont des nombres premiers distincts de* p ;
- *le corps* K *contient les racines* q_1-èmes,...,q_s-èmes *de l'unité ;*
- K' *est une extension cyclique de degré* n *de* K ;
- *Chacun des corps intermédiaires entre* K *et* K' *de degré* $q_i^{e_i}$ *est une extension non ramifiée de* K.

Dans ces conditions :

a- le A*-module bilinéaire* T *est un espace hyperbolique de type fini ;*

b- tout élément de T *s'écrit d'une manière unique sous la forme* $x=y+z$ *avec* $Tr_{K'/K}(y^2) = Tr_{K'/K}(z^2) = 0$.

Soient E_i, i=1,...,s,les corps intermédiaires entre K et K' de degrés $q_i^{e_i}$, i=1,...,s. L'extension E de K est isomorphe au produit tensoriel des E_i qui sont des extensions cycliques K.G. de K. Désignons par A'_i la fermeture intégrale de A dans E_i , i=1,...,s. Comme A est non ramifié dans chaque A'_i, A est non ramifié dans A' et $A' = \bigotimes_{i=1}^{s} A'_i$ (Théorème 3.2).

Pour tout indice i=1,...,s, le sous-A-module T_i des éléments de trace nulle de A_i' est un espace hyperbolique de rang $q_i^{e_i} - 1$ (Théorème 4.2) tel que $A_i' = A \perp T_i$ (Théorème 3.1., corollaire). Nous avons donc

$$A' = \bigotimes_{i=1}^{s} A_i' = \bigotimes_{i=1}^{s} (A \oplus T_i) = A \perp \left(\bigotimes_{i=1}^{s} T_i \right) \perp \left(\perp_{i=1}^{s} T_i \right).$$

Ce qui montre que le sous A-module T des éléments de trace nulle de A' est $T = \left(\bigotimes_{i=1}^{s} T_i \right) \perp \left(\perp_{i=1}^{s} T_i \right)$. D'autre part, nous savons qu'un produit tensoriel (respectivement une somme directe) d'espaces hyperboliques est un espace hyperbolique. Il en résulte que T est un espace hyperbolique de type fini.

COROLLAIRE. - *Les A-modules* A' *et* T *sont libres de rang* n *et* n-1.

b) Extensions cycliques du type de Kummer de degré pair.

On suppose n inversible dans l'anneau A.

THEOREME 4.4. - *Soit* K' *une extension cyclique non ramifiée K.S. de degré pair de* K ; *l'extension* K' *de* K *est engendrée par une racine d'un polynôme irréductible de* K[X] *de la forme* $X^n - a$, *où* $a \in A$.

a - Si A' *est un* A*-module libre, alors tout élément de* T *s'écrit d'une manière unique sous la forme* $x = y + z + \lambda u$, $\lambda \in A$, *avec* $Tr_{K'/K}(y^2) = Tr_{K'/K}(z^2) = 0$ *et* $Tr_{K'/K}(u^2)$ *inversible dans* A.

b- Si -a *est un carré dans* A, *alors* A' *et* T *sont des* A-*modules libres.*

Si -a *n'est pas un carré dans* A, *alors* A' *et* T *sont sommes directes orthogonales d'un* A-*module libre et d'un même* A-*module* R *projectif de rang* 1, *fortement non isotrope et tel que* C(R)=C(A').

Le fait que K' puisse être engendré par une racine d'un polynôme irréductible de K[X] de la forme X^n-a, a $\in$ A, résulte du théorème 2.3. Le A-module A' se décompose sous la forme A' = A $\perp$ T et T est un A-module projectif de rang n-1 et un A-module bilinéaire non dégénéré. L'espace vectoriel K' $\otimes_A$ T n'est autre que le sous-espace vectoriel des éléments de trace nulle de K' ; c'est donc un espace vectoriel bilinéaire non dégénéré d'indice $\frac{n}{2}$ - 1 (prop. 2.7, corollaire). Par suite, T est un A-module bilinéaire non dégénéré d'indice $\frac{n}{2}$ - 1 (prop. 1.8). Le A-module T admet une décomposition de Witt sous la forme T = (N $\oplus$ P) $\perp$ R, où N et P sont des facteurs directs totalement isotropes maximaux et R un facteur direct fortement non isotrope projectif de rang 1. Comme N $\oplus$ P est un espace hyperbolique de type fini sur l'anneau de Dedekind A, c'est un A-module libre de rang fini et nous avons C(T)=C(N$\oplus$P)+C(R)=C(R) et C(A')=C(A)+C(T)=C(T) ; d'où C(T)=C(A')=C(R).

a- Si A' est un A-module libre, alors C(T)=C(A')=C(R)=0 (Théorème 1.3, lemme 1). Ainsi T est un A-module libre de rang n-1 et R un A-module libre de rang 1, fortement non isotrope. Nous en déduisons l'existence d'un

élément u de A' tel que $Tr_{K'/K}(u^2)$ soit inversibl dans A, et que $R = A.u$.

b- Si (-a) est un carré dans A, K' est alors un espace vectoriel bilinéaire non dégénéré d'indice $\frac{n}{2}$, donc un espace hyperbolique (prop. 2.7). Ainsi, A' est un espace hyperbolique de type fini sur A (prop. 1.8), donc un A-module libre (Théorème 2.3) et par suite T est aussi un A-module libre de rang n-1 (Théorème 3.3). Si (-a) n'est pas un carré dans A, K' est alors un espace vectoriel bilinéaire non dégénéré d'indice $\frac{n}{2}-1$ (prop. 2.7). Dans ce cas, la décomposition de A' sous la forme $A' = A \perp T = A \perp [(N \oplus P) \perp R] = [A \perp (N \oplus P)] \perp R$ montre que A' et T sont sommes directes orthogonales d'un A-module libre et d'un même facteur direct R, projectif, de rang 1, fortement non isotrope tel que $C(R) = C(A')$.

COROLLAIRE. - *Si* (-a) *est un carré dans* A, *il existe un élément* $x \neq o$ *de* A *tel que* $Tr_{K'/K}(x) = o$ et $Tr_{K'/K}(x^2)$ *sont inversibles dans* A.

REMARQUE. - Nous nous proposons de montrer qu'il existe des extensions cycliques K.S. non ramifiées de K pour lesquelles T n'est pas un A-module libre.

On considère l'extension quadratique $K=\mathbb{Q}(e)$ du corps des rationnels par $e = \sqrt{-41}$ et on désigne par A le sous-anneau constitué par les éléments de la forme a+be, où a et b sont des élément de l'anneau $B = \mathbb{Z}[\frac{1}{2}]$, anneau

de fractions de $\mathbb{Z}$ défini par la partie multiplicative $S = \{2^n, n \in \mathbb{Z}\}$.

. L'anneau A est la fermeture intégrale de l'anneau principal B dans K ; c'est donc un anneau de Dedekind.

Soit $\mathfrak{a}$ l'idéal de A engendré par 1+e et 3 ; l'idéal $\mathfrak{b} = \mathfrak{a}^2$ est engendré par les éléments $(1+e)^2$, $3(1+e)$ et 9 ; mais $3(1+e)=\frac{3}{2}(1+e)^2+7\ 9$; donc $\mathfrak{b}$ peut être engendré par les éléments $e_1=2-e$; $e_2=9$. Montrons que l'idéal $\mathfrak{b}$ n'est pas principal. A cet effet, considérons l'application

$N: A \longrightarrow B \mid N(a+be) = a^2+41b^2$ et appelons norme de l'élément a+be de A l'image de a+be par cette application. On a en particulier :

$N[(a+be)(c+de)] = N(a+be)N(c+de)$.

Pour un élément a+be de $\mathfrak{b}$, on a :

$a+be=(\alpha+\beta e)e_1+(\gamma+\delta e)\ e_2 = (2\alpha+41\beta+9\gamma)+(-\alpha+2\beta+9\delta)e$, $\alpha, \beta, \gamma, \delta \in B$;

$N(a+be)=(2\alpha+41\beta+9\gamma)^2+41(-\alpha+2\beta+9\delta)^2=9(5\alpha^2+205\beta^2+9\gamma^2+369\delta^2+4\alpha\gamma-82\alpha\delta+82\beta\gamma+164\beta\delta)$;

d'où $N(a+be) \equiv 0 \pmod 9$ dans B.

Supposons $\mathfrak{b}$ principal et soit $t \in A$ un élément générateur; $\mathfrak{b} = At$ et $N(t) \equiv 0 \pmod 9$. Posons $e_1=\alpha t$, $e_2=\beta t$. Il vient : $N(e_1)=N(\alpha).N(t)=45$, $N(e_2)=N(\beta).N(t)=81$; donc $45 \equiv 0 \pmod{N(t)}$, $81 \equiv 0 \pmod{N(t)}$; d'où $9 = 2\ 45-81 \equiv 0 \pmod{N(t)}$.

Les relations $\begin{cases} 9 \equiv 0 \pmod{N(t)}, \\ N(t) \equiv 0 \pmod 9 ; \end{cases}$ entrainent $\begin{cases} 9=\gamma N(t)\ ,\ \gamma \in B\ ,\ \gamma>0, \\ N(t)=9\delta\ ,\ \delta \in B\ ,\ \delta>0\ ; \end{cases}$

d'où $\gamma\delta = 1$.

Or $\gamma = \frac{r}{2^n} > 0$, $\delta = \frac{s}{2^p} > 0$; donc $\frac{rs}{2^{n+p}} = 1$ et, par suite, $r = 2^{m'}$, $s = 2^{p'}$ avec $m'+p' = m+p$. Ainsi $\delta = \frac{1}{2^n}$, $n \in \mathbb{Z}$ et $N(t) = \frac{9}{2^n}$, $n \in \mathbb{Z}$.

On en déduit que $N(\alpha) = 5\ 2^n$, $n \in \mathbb{Z}$. Posant $\alpha = x+ye$, $x,y \in B$, la relation précédente signifie que l'équation : $x^2+41y^2 = 5 \times 2^n$, $n \in \mathbb{Z}$, possède des solutions dans l'anneau B. Or ceci est impossible comme le montre le raisonnement suivant.

Si l'équation $x^2+41y^2 = 5 \times 2^n$ $(n \in \mathbb{Z})$ possédait une solution dans B, il existerait des valeurs entières positives ou nulle de n pour lesquelles l'équation $x^2+41y^2 = 5\ 2^n$ (1) aurait des solutions dans $\mathbb{Z}$. Pour $n=0,1,2,3,4$, on constate sans difficulté que (1) n'a pas de solution. Il reste à examiner s'il existe des valeurs de n entières et supérieures ou égale à 5 pour lesquelles (1) admet des solutions entières. Toute relation de cette équation est nécessairement constituée par des nombres pairs car, modulo 4, le second membre est nul. Supposons qu'une telle solution existe et posons $x = 2x_1$, $y = 2y_1$. L'équation $x^2+41y^2 = 5 \times 2^{n-2}$ admet la solution (x_1, y_1). En itérant le procédé, on arrive à la conclusion suivante : $x^2+41y^2 = 5 \times 2^n$, $n < 5$ admet des solutions, ce qui est impossible.

Par contre, l'idéal $\mathfrak{b}^2 = \mathfrak{a}^4$ est principal. Il est engendré par les éléments $(2-e)^2$, $9(2-e)$ et 81. Or $9(2-e)-2(2-e)^2-81 = 11-e$; donc $11-e$ est un élément de $\mathfrak{b}^2$. Il est facile de vérifier que les éléments $(2-e)^2$, $9(2-e)$ et 81 appartiennent à l'idéal $A(11-e)$; donc $\mathfrak{b}^2 = A(11-e)$.

Les éléments 11+e et -(11+e) ne sont pas des carrés dans $\mathbb{Q}(\sqrt{-41})$; on désigne par E l'extension quadratique de $\mathbb{Q}(\sqrt{+41})$ par une racine du polynôme $X^2-(11+e)$ et par A' la fermeture intégrale de A dans E.

$z \in E \Leftrightarrow z = u+vx$, $u,v \in K$; $x^2 = 11+e$.

$$z=\alpha+\beta x \in A' \Rightarrow \bar{z}=\alpha-\beta x \in A' \Rightarrow \begin{cases} z+z = 2\alpha \in A \\ z\bar{z}=\alpha^2-\beta^2(11+e) \in A \end{cases} \rightarrow \begin{cases} \alpha \in A \\ \alpha^2-\beta^2(11+e) \in A \end{cases} \Rightarrow \alpha \in A, \beta^2(11+e) \in A.$$

Ces conditions sont nécessaires pour que l'élément $z = \alpha+\beta x$ de E appartienne à A', elles sont aussi suffisantes, car alors z est racine de $x^2-2\alpha x + \alpha^2-\beta^2(11+e) = 0$.

Soit T l'ensemble des éléments de trace nulle dans A' ; alors $T = \{ \beta x,\ \beta \in K \mid \beta^2(11+e) \in A \}$. Nous nous proposons de déterminer complètement le sous-A-module T.

Posons $\beta = u+ve$; $u,v \in Q$. On a :

$$\beta^2(11+e)=(u+ve)^2(11+e)=(u^2-41v^2+2uve)(11+e)=11(u^2-41v^2)-82uv+[u^2-41v^2+22uv]e ;$$

$$\beta^2(11+e) \in A \Rightarrow \begin{cases} 11(u^2-41v^2)-82uv \in B , \\ u^2-41v^2+22uv \in B. \end{cases}$$

Considérons le système (I) $\begin{cases} 11(u^2-41v^2)-82uv \in B & (1), \\ u^2-41v^2+22uv \in B & (2). \end{cases}$

(I) $\Longrightarrow$ (II) $\begin{cases} 81\ uv \in B & (1'), \\ 81(u^2-41v^2) \in B & (2'). \end{cases}$

En multipliant (1') et (2') par une même puissance convenable de 2, on voit que :

$$(I)\Longrightarrow(II)\quad \begin{cases} 2^m\, 81uv = \lambda \qquad (1''), \\ 2^m\, 81(u^2-41v^2) = \mu \quad (2''), \end{cases} \qquad (\lambda,\mu \in \mathbb{Z}).$$

Si $u = p/q$ est une représentation irréductible de u, alors $q=2^n s$, où s est un diviseur de 81; donc $81 = st$; s peut prendre les valeurs 1,2,9,27,81. Tirant v de (1") et portant dans (2), il vient toutes réductions faites :

$$2^{2m}t^2p^4 + 2^{m+2n}st\,p^2(22\lambda - 2^m 81v) - 41\times 2^{4n}\lambda^2 s^2 = 0\ ,\ v \in B.$$

Il en résulte que s divise t^2; donc s ne peut prendre que les valeurs 1,3,9. Finalement, u se met sous la forme $u = \dfrac{r}{2^n 9}$, $r \in \mathbb{Z}$.

Utilisant (2"), il vient alors : $v = \dfrac{r'}{2^n 9}$, $r' \in \mathbb{Z}$.

Exprimons enfin que ces valeurs de u et v sont solutions du système (I), ce qui revient à écrire que, modulo 81, r et r' satisfont au système :

$$(IV)\quad \begin{cases} 11(r^2-41r'^2)-rr' = 0, \\ r^2-41r'^2+22rr' = 0, \end{cases}$$

qui se réduit à la seule équation $(r+11r')^2 \equiv 0 \pmod{81}$, équivalente à $r+11r' \equiv 0 \pmod 9$.

La solution générale du système (I) est donnée par $\beta = \dfrac{9k-11l}{9\times 2^n} + \dfrac{l}{9\times 2^n}$, $k, l \in \mathbb{Z}$.

Or $\beta = \frac{k-\ell}{2^n} - \frac{\ell}{2^n}.\frac{2-e}{9}$; les éléments β constituent un idéal fractionnaire de K engendré par les éléments 1 et $\frac{2-e}{9}$; cet idéal est isomorphe à l'idéal entier $\mathfrak{b}$ de A par l'isomorphisme de A-modules $\sigma : \beta \mapsto \gamma = 9\beta$. De ces différentes remarques, il résulte que le A-module T est isomorphe au A-module $\mathfrak{b}$; par conséquent T est un A-module projectif de rang 1 qui n'est pas sur A-module libre.

D'autre part, considérons la forme bilinéaire B sur T×T définie par $(\beta,\beta') \mapsto \mathrm{Tr}_{E/K}\ \beta\beta' x^2 = 2\beta\beta'(11+e)$ et effectuons l'isomorphisme de A-modules σ, qui au A-module bilinéaire (T,B) associe le A-module bilinéaire $(\mathfrak{b}, B')$ avec $B'(\gamma,\gamma') = B'(\sigma(\beta),\sigma(\beta')) = B(\beta,\beta') = 2\beta\beta'(11+e)$,

$$B'(\gamma,\gamma') = \frac{2(11+e)}{81}\gamma\gamma'$$

L'idéal $\mathfrak{b}^{-2}$ est engendré par l'élément $(11-e)^{-1}$ et $\frac{2(11+e)}{81} = 4(11-e)^{-1}$; il en résulte que les formes bilinéaires B' et B sont non dégénérées.

Nous avons ainsi un exemple d'une extension du type de Kummer simple, non ramifiée par une racine d'un polynôme de la forme $X^n - a$, avec -a non carré dans A, et pour laquelle T n'est pas un A-module libre.

THEOREME 4.5. - *Soit* K' *une extension cyclique K.S. non ramifiée de degré* $n = 2^e$ *de* K. *Soit* F_1 *le corps intermédiaire de rang* 2^{e-1} *entre* K *et* K' ; *on suppose que* K' *est engendré sur* F_1 *par une racine d'un polynôme de la forme* $X^p - a_1$, *avec* $a_1 \in F$ *et que* $(-a_1)$ *est*

carré dans F_1.

Alors, les A*-modules* A' *et* T *sont libres.*

L'hypothèse "$(-a_1)$ carré dans F_1" implique que K' est un plan hyperbolique sur F_1. Il existe alors un sous-F_1-espace vectoriel N_1 de K' totalement isotrope et de rang 1 ; donc N_1 est un K-espace vectoriel totalement isotrope de rang 2^{e-1}. Par suite, K' est un K-espace hyperbolique. Il en résulte que A' est aussi un espace hyperbolique sur A, donc un A-module libre. Le A-module T est alors libre.

REMARQUE. - Considérons la situation suivante :

$A = \left\{a+be \ ; \ a,b \in \mathbb{Z}\left(\frac{1}{2}\right)\right\}$, $K = \mathbb{Q}(e)$, $K'=K(x)$, $x^2=11+e$, $K'' = K'(i)$.

L'extension K" de K est une extension cyclique K.G. de degré 4. Les extensions K' de K et K" de K' sont non ramifiées, donc K" est une extension non ramifiée de K. D'autre part, 1 étant carré dans A, la fermeture intégrale A" de A dans K" est un A-module libre de rang 4. Enfin A" étant aussi la fermeture intégrale de A' dans K", A" est un A'-module libre. Ainsi les propositions :

"$A \subset A' \subset A$" ; A" est A-module libre ; A" est A'-module libre".

n'impliquent pas "A' est A-module libre".

BIBLIOGRAPHIE.

N. BOURBAKI, *Algèbre Commutative*, Chap. V.

M. FLAMANT et L. HENOUD, *Bull. Soc. Math. Fr.* , 97 (1969), p. 299-307.

L. HENOUD, *Thèse de 3e cycle*, Lyon (1973).

L. HENOUD , M. FLAMANT
Centre d'Etudes et de Recherches
mathématiques et physiques
B.P. 3855
BEYROUTH (Liban)