UNIVERSITAT DE BARCELONA

Sobre la parte *P*-fundamental del grupo de Brauer

Josep Vaquer i Timoner

Mat.

SOBRE LA PARTE P-FUNDAMENTAL DEL GRUPO DE BRAUER

POR

JOSE VAQUER TIMONER

MEMORIA PRESENTADA PARA ASPIRAR AL GRADO DE DOCTOR EN CIENCIAS (SECCION DE MATEMATICAS)

José Vaquer

Juan Augé

PROLOGO

Según un conocido teorema de Wedderburn (*), toda álgebra normal y simple es el producto directo (tensorial) de un álgebra total de matrices y un álgebra de división. A partir de aquí R. Brauer divide las álgebras normales y simples en clases y define en el conjunto de clases una extructura de grupo abeliano (**).

En el caso que el cuerpo de coeficientes sea de característica p>0, el estudio de la parte p-fundamental del grupo de Brauer de clases de álgebras se reduce al de las p-álgebras cíclicas (***) que fueron estudiadas por E. Witt en 1936 (****) y al mismo tiempo O. Teichmüller obtenia algunas relaciones entre las p-álgebras ciclicas con respecto a la clasificación de Brauer (*****).

Recientemente E. Witt (++++++) ha dado un isomorfismo entre la parte p-fundamental del grupo de Brauer de clases

---

(*) Wedderburn [6] ; véase también A. Albert [1] th. 3.9.

(**) R. Brauer [2] ; véase también A. Albert [1] th. 4.19.

(***) A. Albert [1] th. 7.31. y th. 5.17.

(****) E. Witt [7]

(*****) O. Teichmüller [4] y [5]

(++++++) E. Witt [8]

de álgebras y un módulo de formas de Pfaff en el que se calcula con gran fluidez y permite dar un sistema de generadores de la parte p-fundamental del grupo de Brauer a partir de una p-base del cuerpo de coeficientes.

Las relaciones entre las p-álgebras cíclicas obtenidas por O. Teichmüller dan los generadores nulos y algunas relaciones de forma muy particular. El objeto de este trabajo es obtener <u>todas</u> las relaciones entre los generadores anteriormente citados. Este problema se resuelve primeramente trabajando en el módulo de formas de Pfaff (§ 5), y después, siguiendo los mismos métodos de Teichmüller, independientemente del módulo de formas de Pfaff (§ 6).

Para los teoremas generales sobre álgebras usados en este trabajo puede verse el libro de A. Albert [1]. Para facilitar la lectura se empieza con un resumen del cálculo vectorial de Witt (§ 1) y su aplicación a la obtención de las p-álgebras cíclicas sobre un cuerpo k (§ 2), y finalmente el isomorfismo entre la parte p-fundamental del grupo de Brauer de clases de álgebras y un módulo de formas de Pfaff sobre el anillo de vectores de Witt (§ 3).

El tema del presente trabajo me fué propuesto durante mi estancia en Hamburgo (1956/58) por el Profesor E. Witt

al que expreso mi agradecimiento tanto por la ayuda que me ha prestado durante la ejecución del mismo como por todas las enseñanzas de él recibidas. Expreso también mi agradecimiento al Dr. J. Augé por el apadrinamiento de esta tesis y al C.S.I.C. y a D.A.A.D. que me proporcionaron la beca que me permitió realizar estos estudios.

§ 1. Cálculo vectorial de Witt (*).

Sea p un número primo fijo. Para cada vector

$$x = (x_o, x_1, \ldots\ldots)$$

con una infinidad numerable de componentes, cuya naturaleza por el momento no interesa especificar, se definen las componentes secundarias

$$\text{(a)} \qquad x^{(n)} = x_o^{p^n} + p x_1^{p^{n-1}} + \ldots + p^n x_n$$

polinomios enteros en las componentes principales, y si interesa se escriben explicitamente en el vector

$$x = (x_o, x_1, \ldots | x^{(o)}, x^{(1)}, \ldots).$$

Las igualdades (a) permiten calcular las componentes principales x_i como polinomios racionales en las componentes secundarias $x^{(i)}$, y un vector queda determinado tanto por las componentes principales como por las secundarias.

Se define la suma, diferencia y producto de dos vectores efectuando dichas operaciones en las componentes secundarias, es decir:

(*) Vease Witt [7]

$$\text{(b)} \quad (x_0,x_1,\ldots|x^{(o)},x^{(1)},\ldots) \dot{\pm} (y_0,y_1,\ldots|y^{(o)},y^{(1)},\ldots) =$$
$$= (?,?,\ldots|x^{(o)} \dot{\pm} y^{(o)},x^{(1)} \dot{\pm} y^{(1)},\ldots).$$

Para estudiar las operaciones anteriormente definidas se introducen los operadores

$$(1) \qquad T(x_0,x_1,\ldots) = (0,x_0,x_1,\ldots)$$

$$(2) \qquad P(x_0,x_1,\ldots) = (x_0^p,x_1^p,\ldots)$$

$$(3) \qquad \wp(x_0,x_1,\ldots) = P(x_0,x_1,\ldots) - (x_0,x_1,\ldots)$$

y las abreviaciones

$$(4) \qquad \{u\} = (u,0,0,\ldots)$$

que si no hay confusión posible se escribe u en vez de $\{u\}$.

$$0 = (0,0,0,\ldots.)$$
$$(5) \qquad 1 = (1,0,0,\ldots.)$$
$$m = 1 + 1 + \ldots + 1 \quad (m \text{ sumandos})$$

y se verifica:

$$(6) \qquad T(x + y) = Tx + Ty$$

$$(7) \qquad (x_0,x_1,\ldots) = \sum_{i=0}^{r-1} T^i \; x_i \; + T^r(x_r,x_{r+1},\ldots)$$

$$(8) \qquad \{u\}(x_0,x_1,\ldots) = (ux_0,u^p x_1,u^{p^2} x_2,\ldots)$$

como se comprueba facilmente escribiendo las componentes secundarias

Se demuestran (Witt [7]) los dos teoremas siguientes:

Teorema 1.- La componente (n+1)-sima, $(x \dot{\pm} y)_n$, de $(x_o, x_1, \ldots) \dot{\pm} (y_o, y_1, \ldots)$ es un polinomio entero en $x_o, x_1, \ldots x_n, y_o, y_1, \ldots, y_n$.

Teorema 2.- $(px)_n \equiv (TPx)_n$ mód.$pG[x_i]$ (G enteros)

El teorema 1 nos muestra que las operaciones $\dot{\pm}$ definidas mediante las componentes secundarias, pueden también definirse mediante polinomios enteros (en general complicados) en las componentes principales sin mencionar para nada de las componentes secundarias, con lo que (1),..,(8) y los teoremas 1 y 2 siguen valiendo, y las propiedaddes asociativa, conmutativa y distributiva son consecuencia de identidades entre estos polinomios.

Desde este punto de vista pueden considerarse los polinomios enteros,que definen las operaciones, módulo p con lo que (1),...,(8) conservan su validez y los teoremas 1 y 2 se convierten en los siguientes:

Teorema 1.- $(x + y)_n$ es un polinomio en $x_o, \ldots, x_n$, $y_o, \ldots, y_n$ con coeficientes del cuerpo primo de característica p.

Teorema 2.- $px = TPx = PTx$

Además se verifica (Witt [7])

(9) $P(x \dot{\pm} y) = Px \dot{\pm} Py$

(10) $(T^i x)(T^j y) = T^{i+j}(P^j x . P^i y)$

Sea ahora k un cuerpo de caracteristica p. Si se consideran los vectores cuyas componentes son elementos de k, éstos forman un anillo $W(k)$.

En el anillo $W(k)$ se puede definir una valoración por $|x| = p^{-r}$ si x_r es la primera componente de x distinta de 0, $|0| = 0$.

De (10) y (6) se sigue:

(11) $|x + y| \leqq \text{máx.}(|x|, |y|)$

(12) $|xy| = |x| \cdot |y|$.

Con esta valoración se puede hablar de convergencia y (7) se convierte en

(13) $(x_0, x_1, \ldots) = \sum_{i=0}^{\infty} T^i \{x_i\} = \sum_{i=0}^{\infty} P^{-i}\{x_i\} p^i$.

Teorema 5.- (*) En el anillo $W(k)$ los elementos que tienen inverso son los que tienen la primera componente distinta de cero.

Si $x = (x_0, x_1, \ldots)$ entonces $x^{-1} = \{x_0^{-1}\} \sum_{i=0}^{\infty} (1 - x\{x_0^{-1}\})^i$.

(*) En los teoremas se sigue la misma numeración de Witt [7]

§ 2 p-álgebras cíclicas (*).

El anillo de vectores $W(k)$ anteriormente definido permite obtener todos los cuerpos cíclicos de grado p^n y p-álgebras cíclicas sobre el cuerpo k (**).

Para ello se calcula en el anillo $W(k)$ módulo T^n (o brevemente con vectores de longitud n).

Sea $a \neq 0$ un elemento de k y $b = (b_o, \ldots, b_{n-1})$ un vector de longitud n de $W(k)$. La expresión

$$(a|b]_n = (a|b_o, \ldots, b_{n-1}]_n$$

designa el álgebra sobre k engendrada por $u, v_o, \ldots, v_{n-1}$ con las relaciones

$$u^{p^n} = a \, , \quad \wp v = b \, , \quad u\, v\, u^{-1} = v + 1 \, , \quad v_i v_j = v_j v_i$$

donde

$$v = (v_o, \ldots, v_{n-1}) \quad y \quad u\, v\, u^{-1} = (u v_o u^{-1}, \ldots, u v_{n-1} u^{-1})$$

y se tiene (Witt [7])

<u>Teorema</u>.- $(a|b]_n$ es un álgebra normal y simple de grado p^n ( ) sobre k , y es semejante a una p-álgebra cíclica. Reciprocamente toda p-álgebra cíclica es de la forma $(a|b]_n$.

(*) Witt [7]

(**) Albert [1]

Como es sabido (*) toda álgebra normal y simple es producto directo (tensorial) de un álgebra total de matrices y un álgebra de división, y esta descomposición está determinada salvo isomorfismos internos del álgebra. Dos álgebras se llaman semejantes si las álgebras de división correspondientes son isomorfas. La semejanza es una relación de equivalencia que permite clasificar las álgebras normales y simples en clases. En el conjunto de clases se puede definir una operación (que escribimos aditivamente: la clase suma es la que contiene el producto directo de dos representantes de los sumandos) respecto de la cual forma un grupo conmutativo llamado grupo de Brauer de clases de álgebras. La parte p-fundamental (× ×) está formada por las clases que contienen una p-álgebra cíclica o sea según el teorema anterior, algebras de la forma $(a|b]_n$

En este grupo se verifica (× × ×):

(1) $$(a|b]_n + (a'|b]_n = (aa'|b]_n$$

(2) $$(a|b]_n + (a|b']_n = (a|b + b']_n$$

(×) Albert [1]

(× ×) Subgrupo de elementos de orden una potencia de p

(× × ×) Witt [7]

(3) $p^n(a|b]_n = 0$

(4) $(a|Pb]_n = (a|b]_n = (a|Tb]_{n+1}$

(5) $(a|b^{p^n}a^r,0,\dots,0]_n = 0$ si $m.c.d.(p,r)=1$ (x)

Nótese que la igualdad $(a|Pb]_n = (a|b]_n$ permite definir $(a|b]_n$ como elemento del grupo de Brauer de clases de álgebras para cualquier

$$b \in W(k^{p^{-m}}).$$

(x) Teichmüller [5]

§ 3. Expresión de las p-álgebras cíclicas mediante formas de Pfaff (×).

El cálculo de la parte p-fundamental del grupo de Brauer de clases de álgebras viene grandemente facilitado por el isomorfismo de esta parte p-fundamental con un módulo cociente del módulo de formas de Pfaff formales sobre el anillo

$$W = \bigcup_{h=0}^{\infty} W(k^{p^{-n}}).$$

Sea k un cuerpo, de característica p . H_{Ω} la parte p-fundamental del grupo de Brauer de clases de álgebras sobre k , que corresponde a las álgebras que se descomponen en

$$\Omega = \bigcup_{h=0}^{\infty} k^{p^{-n}} \quad (\times\times).$$

Sean w_n el anillo de vectores de Witt con componentes de $k^{p^{-n}}$ y $W = \bigcup_{h=0}^{\infty} w_n$. Además sean $W\,dW$ y $w_n\,dw_n$ módulos de formas de Pfaff formales (×××), es decir el módulo de las sumas formales de elementos a db con las reglas:

(×) Witt [8]

(××) Albert [1]

(×××) Kähler [3]

$$(a + a_1)\, db = a\, db + a_1\, db$$

(1) $$a\, d(b + b_1) = a\, db + a\, db_1$$

$$a\, d(bb_1) = ab\, db_1 + ab_1\, db$$

Finalmente dentro de estos módulos de formas de Pfaff se considera el endomorfismo definido por

$$\Pi\ (a\, db) = (Pa\, dPb) - p(a\, db)$$

que como es fácil ver es compatible con las reglas (1).

Para definir el isomorfismo antes indicado se consideran las aplicaciones

$$w_n\ dw_m \dashrightarrow H_\Omega$$

definidas por

$$a\, db = \sum_{i=0}^{m-1} (P^{i+n} a_i | a_i b]_n$$

donde se ha expresado según §1-(13)

$$a = \sum a_i p^i$$

y por tanto

$$a_i \in k^{p^{-n-i}} \quad , \quad P^{i+n} a_i \in k$$

Estas aplicaciones son compatibles con las inclusiones

$$w_o \subset w_1 \subset w_2 \subset \cdots$$

pues si se considera

$$a\, db \in w_{n+1}\, dw_m$$

se tiene

$$a\, db = \sum_{i=0}^{m-1} (P^{i+n+1}a_i \; a_i b \;{}_{n+1}$$

pero llamando $P^{i+n}a_i = c \in k$ y teniendo en cuenta (1), (2) y (4) del §2 se tiene:

$$(P^{i+n+1}a_i | a_i b]_{n+1} = (Pc | a_i b]_{n+1} = (c | pa_i b]_{n+1} =$$

$$= (c | PTa_i b]_{n+1} = (c | a_i b]_n = (P^{i+n}a_i | a_i b]_n \,.$$

Y si se considera

$$a\, db \in w_n\, dw_{m+1}$$

se tiene

$$a\, db = \sum_{i=0}^{m} (P^{i+n}a_i | a_i b]_n$$

pero llamando $P^{m+n}a_m = c \in k$ y teniendo en cuenta (4) y (5) del §2 se tiene

$$(P^{m+n}a_m | a_m b]_n = (c | a_m b]_n = (c | P^{m+n}(a_m b)]_n = (c | cP^{m+n}b]_n$$

pero $b \in w_m$ luego

$$P^{m+n}b = (b_0^{p^n}, \dots, b_{n-1}^{p^n}) \qquad \text{con} \quad b_i \in k$$

y

$$(c | cP^{m+n}b]_n = (c | cb_0^{p^n}, cb_1^{p^n}, \dots, cb_{n-1}^{p^n}]_n = 0$$

Luego estas aplicaciones definen una aplicación

$$W\, dW \dashrightarrow H_{\Omega}$$

en la que $w_o\, dW = 0$, pues si $a \in w_o$ resulta

$$a\, db = \sum (P^{i+1} a_i | a_i b]_1 = 0$$

Esta aplicación es compatible con las reglas (1) de derivación, en efecto:

a) $a\, d(b + b') = a\, db + a db'$ es trivial

b) Si $a = \sum a_i p^i$, $b = \sum b_i p^i$ y $c = \sum c_i p^i \in w_n$

se tiene:

$$a\, d(bc) = \sum_{i,j,k} (P^{i+n} a_i | a_i b_j c_k p^{j+k}]_n =$$

$$= \sum_{i,j,k} (P^{i+j+k+n} a_i | a_i b_j c_k]_n =$$

$$= \sum_{i,j,k} (P^{i+j+k+n} a_i | P^{i+j+k+n}(a_i b_j c_k)]_n$$

luego teniendo en cuenta (1) y (5) del § 2 resulta

(2) $$a\, d(bc) + b\, d(ca) + c\, d(ab) = 0$$

c) Teniendo en cuenta $w_o\, dW = 0$ y haciendo $c = 1$ en (2) resulta:

(3) $$a\, db + b\, da = 0$$

d) De a) y c) resulta que la aplicación es lineal en a.

e) De (2) y (3) resulta

$$a\, d(bc) = ab\, dc + ac\, db.$$

Es decir que esta aplicación es un homomorfismo del módulo $W\, dW$ en H_Ω

En este homomorfismo $\Pi(W\, dW) = 0$ (consecuencia inmediata de (1) y (4) del § 2.

Se demuestran:

<u>Teorema 1.</u>- Si $k \subset k_1 \subset k_2 \subset \dots \subset k_n$ es una sucesión de ampliaciones puramente inseparables de k con $k_i = k(a_1, a_2, \dots, a_i)$ de grado p^i sobre k, y el álgebra A se descompone en k_n, entonces

$$A = \sum_{i=1}^{n} b_i \frac{da_i}{a_i} \qquad \text{con} \quad b_i \in k.$$

De este teorema se deduce inmediatamente que $W\, dW \longrightarrow H_\Omega$ es un epimorfismo.

<u>Teorema 3.</u>- (*) El núcleo del homomorfismo

$$W\, dW \longrightarrow H_\Omega$$

es

$$w_0\, dW + \Pi(W\, dW)$$

(*) La numeración de los teoremas es la de Witt [8]

Se tiene pues el isomorfismo

$$H_{\Omega} \cong W\,dW \,/\, w_o\,dW + \Pi(W\,dW)$$

Para el cálculo conviene tener presentes algunas reglas (en parte ya citadas) deducidas de $w_o\,dW + \Pi(W\,dW) = 0$

(5) $$P(a\,db) = p(a\,db)$$

(6) $$a\,db + b\,da = 0$$

(7) $$w_o\,dW = 0\ ,\ W\,dw_o = 0$$

(8) $$a\,d(Tb) = Pa\,db$$

(9) $$a\,\frac{d\}b\{}{\}b\{} = Pa\,\frac{d\}b\{}{\}b\{} \quad \text{si } b \in \Omega$$

La forma $a\,\dfrac{d\}b\{}{\}b\{}$ se escribe abreviadamente $a\,dlb$.

§ 4. Generadores y relaciones de H_Ω

El teorema 1 del § anterior permite obtener un sistema de generadores de la parte p-fundamental H_Ω del grupo de Brauer de clases de álgebras sobre el cuerpo k de característica p, pues si U es una p-base de k (es decir un subconjunto minimal de k tal que $k = k^p(U)$) y $A \in H_\Omega$, A se descompone en un cierto cuerpo $k(\xi_1, \ldots, \xi_s) = K$ con $\xi_i \in \bigcup_{n=0}^{\infty} U^{p^{-n}}$, y existirá una cadena de cuerpos $k = k_1 \subset k_2 \subset \ldots \subset k_n = K$ en las condiciones del teorema 1 con las a de la forma $\xi_i^{p^r}$, luego según dicho teorema

$$A = \sum b_{i,r} \, \mathrm{dl}\, \xi_i^{p^r} \qquad\qquad \text{con } b_{i,r} \in k$$

o sea

$$A = \sum p^r b_{i,r} \, \mathrm{dl}\, \xi_i = \sum_{i=1}^{s} b_i \, \mathrm{dl}\, \xi_i$$

donde se ha puesto

$$b_i = \sum_r p^r b_{i,r} \in w_o$$

luego podemos enunciar

<u>Teorema 1</u>.- Si U es una p-base de k, la parte p-fundamental H_Ω del grupo de Brauer de clases de álgebras sobre k está engendrada por los elementos $b \, \mathrm{dl}\, \xi$ con $b \in w_o$ y $\xi \in \bigcup_{n=0}^{\infty} U^{p^{-n}}$

Que si se quiere puede enunciarse

Si U es una p-base de k, el módulo

$$W\,dW \,/\, w_0\,dW + \Pi(W\,dW)$$

está engendrado por los elementos $b\,dl\xi$ con $b \in w_0$, $\xi \in \bigcup_{n=0}^{\infty} U^{p^{-n}}$

Si $\xi^{p^n} = a \in U$, el isomorfismo del $\int$ anterior nos da

$$b\,dl\xi = \frac{b}{\{\xi\}}\,d\{\xi\} = -\{\xi\}\,d\frac{b}{\{\xi\}} = -(P^n\xi|\{\xi\}\frac{b}{\{\xi\}}]_n = -(a|b]_n$$

luego el teorema anterior puede enunciarse

<u>Teorema 1</u>'.- Si U es una p-base de k, la parte p-fundamental H_Ω del grupo de Brauer de clases de álgebras sobre k está engendrada por los elementos $(a|b]_n$ con $a \in U$ y $b \in w_0$.

Unas relaciones entre estos generadores vienen dadas por el siguiente teorema de E. Witt (*)

<u>Teorema 2'</u>.- Si a y b son dos elementos de k y $a \notin k^p$, $(a|b]_1 = 0$ si y sólo si existen $c \in k$ y $f_r \in k$ tales que

$$b = \wp c + \sum_{r=1}^{p-1} f_r^p a^r$$

(*) O. Teichmüller [4]

Teorema que enunciado en el módulo de formas de Pfaff según el isomorfismo del § 3 dice

<u>Teorema 2</u>.- Si $\xi^p = a \in k$, $a \notin k^p$, $b \in w_o$, entonces es

$$b \, dl\xi = 0 \quad (\text{mód. } w_o \, dW + \Pi(W \, dW))$$

si ysólo si existen $c \in w_o$ y $f_r \in k$ tales que

$$b = \wp c + \sum_{r=1}^{p-1} \{ f_r^p \, a^r \} \quad (\text{mód. } TW)$$

Aquí, apoyándonos en este teorema, vamos a demostrar en general

<u>Teorema 3</u>.- Si $a_1, a_2, \ldots, a_s$ son p-independientes en k, $\xi_i^{p^n} = a_i$ y $b_i \in w_o$, entonces es

$$\sum_{i=1}^{s} b_i \, dl\xi_i = 0 \quad (\text{mód. } w_o \, dW + \Pi(W \, dW))$$

si y sólo si existen $c_i \in w_o$ y $f_{r_1,\ldots,r_s} \in k$ tales que

$$b_i = \wp c_i + \sum_{r_1,\ldots,r_s=0}^{p^n-1} r_i \{ f_{r_1,\ldots,r_s}^{p^n} \, a_1^{r_1} \ldots a_s^{r_s} \} \quad (\text{mód. } T^n W)$$

o bien teniendo en cuenta el isomorfismo definido en el § 3, se puede enunciar

<u>Teorema 3'</u>.- ( ) Si $a_1,\dots,a_s$ son p-independientes en k y $b_i \in W_o$, entonces es

$$\sum_{i=1}^{s} (a_i | b_i]_n = 0$$

si ysólo si existen $c_i \in W_o$ y $f_{r_1,\dots,r_s} \in k$ tales que

$$b_i = \wp c_i + \sum_{r_1,\dots r_s=0}^{p^k-1} r_i \left\{ f^{p^n}_{r_1,\dots,r_s} a_1^{r_1} \dots a_s^{r_s} \right\} \quad (\text{mód.}\, T^n W)$$

Teniendo en cuenta $b\, dl\,\xi^p = pb\, dl\,\xi$ o (4) del §2 se ve inmediatamente que estos teoremas nos dan todas las relaciones entre los generadores de H_Ω dados por el teorema 1.

Estos dos últimos teoremas son los fundamentales demostrados en este trabajo, se dan dos demostraciones independientes, en el fondo equivalentes mediante el isomorfismo del §3.

Empezamos por el teorema 3 que se demuestra por inducción sobre n y s, y al que dividiremos en varias proposiciones parciales. Después pasamos a la demostración del teorema 3' independientemente del módulo de formas de Pfaff siguiendo los mismos métodos que usó Teichmüller para demostrar los casos particulares $n = 1$ [4] y $s = 1$ [5]

§ 5. Demostración del teorema 3.

Si $a_1,\dots,a_s$ son elementos p-independientes de k, $f_{r_1,\dots,r_s} \in k$ y

$$f = \sum_{r_1,\dots,r_s=0}^{p^n-1} \{ f^{p^n}_{r_1,\dots,r_s} \; a_1^{r_1}\dots a_s^{r_s} \} \in W$$

escribiremos abreviadamente

$$\frac{\partial f}{\partial l a_i} = \sum_{r_1,\dots,r_s=0}^{p^n-1} r_i \{ f^{p^n}_{r_1,\dots,r_s} \; a_1^{r_1}\dots a_s^{r_s} \} \in W$$

Proposición 1 (teorema directo).- Si los vectores b_i son de la forma

$$b_i = \delta \, c_i + \frac{\partial f}{\partial l a_i} \qquad (\text{mód. } T^n W)$$

con $a_1,\dots,a_s$ p-independientes en k, $c_i \in W_o$, $f_{r_1,\dots,r_s} \in k$, y

$$f = \sum_{r_1,\dots,r_s=0}^{p^n-1} \{ f^{p^n}_{r_1,\dots,r_s} \; a_1^{r_1}\dots a_s^{r_s} \}$$

y si $\xi_i^{p^n} = a_i$, entonces es

$$\sum_{i=1}^{s} b_i \, dl\xi_i = 0 \qquad (\text{mód.} w_o \, dW + \Pi(W \, dW))$$

Demostración. Por la linealidad en b basta demostrar:

a) $\delta \, c_i \, dl\xi_i = 0$, b) $T^n b_i \, dl\xi_i = 0$, c) $\displaystyle\sum_{i=1}^{s} \frac{\partial f}{\partial l a_i} dl\xi_i = 0$

a) es consecuencia inmediata de (9) del § 3.

b) Por (5) del §3 es

$$T^n b_i\, dl\xi_i = (p^n P^{-n} b_i)\, dl\xi_i = b_i\, dla_i$$

que según (7) del §3 es 0.

c) Por (9) del §3 podemos escribir

$$\sum_{i=1}^{s} \frac{\partial f}{\partial la_i}\, dl\xi_i = \sum_{\substack{i=1,\dots,s \\ r_1,\dots,r_s=0,\dots,p^n-1}} r_i \left\{ f^{p^n}_{r_1,\dots,r_s}\, a_1^{r_1}\dots a_s^{r_s} \right\} dl\xi_i =$$

$$= \sum_{\substack{i=1,\dots,s \\ r_1,\dots,r_s=0,\dots,p^n-1}} r_i \left\{ f_{r_1,\dots,r_s}\, \xi_1^{r_1}\dots \xi_s^{r_s} \right\} dl\xi_i$$

y por (7) del §3

$$\sum_{i=1}^{s} \frac{\partial f}{\partial la_i}\, dl\xi_i = \sum_{\substack{i=1,\dots,s \\ r_1,\dots,r_s=0,\dots,p^n-1}} r_i \left\{ f_{r_1,\dots,r_s}\, \xi_1^{r_1}\dots \xi_s^{r_s} \right\} dl\xi_i +$$

$$+ \sum_{r_1,\dots,r_s=0,\dots,p^n-1} \left\{ \xi_1^{r_1}\dots \xi_s^{r_s} \right\} df_{r_1,\dots,r_s}$$

y teniendo en cuenta la regla de derivación

$$\sum_{i=1}^{s} \frac{\partial f}{\partial la_i}\, dl\xi_i = \{1\}\, d \sum_{r_1,\dots,r_s=0,\dots,p^n-1} \left\{ f_{r_1,\dots,r_s}\, \xi_1^{r_1}\dots \xi_s^{r_s} \right\}$$

luego por (7) del §3

$$\sum_{i=1}^{s} \frac{\partial f}{\partial la_i}\, dl\xi_i = 0$$

<u>Proposición 2</u> (teorema reciproco para $n = 1$).- Si $a_1,\dots,a_s$ son elementos p-independientes de k, $\xi_i^p = a_i$, $b_1,\dots,b_s$ vectores de W_o y

$$\sum_{i=1}^{s} b_i \, dl\xi_i = 0 \quad (\text{mód. } W_o \, dW + \eta(W\, dW)),$$

entonces existen vectores $c_1,\dots,c_s$ de W_o y elementos $f_{r_1,\dots,r_s} \in k$ tales que

$$b_i = \wp c_i + \frac{\partial f}{\partial la_i} \quad (\text{mód. } TW)$$

con

$$f = \sum_{r_1,\dots r_s = 0,\dots,p-1} \{ f^p_{r_1,\dots,r_s} \; a_1^{r_1}\dots a_s^{r_s} \}$$

Demostración por inducción sobre s. Para $s = 1$ es el teorema2. Supongamos la proposición cierta para $1,\dots,s-1$, y sea $K = k(\xi_1,\dots,\xi_{s-1})$ el cuerpo obtenido por adjunción de $\xi_1,\dots,\xi_{s-1}$ a k, entonces

$$\sum_{i=1}^{s-1} b_i \, dl\xi_i \in W(K)\, dW$$

luego

$$b_s \, dl\xi_s = \sum_{i=1}^{s} b_i \, dl\xi_i = 0 \quad (\text{mód.} W(K)\, dW + \eta(W\, dW))$$

y según el teorema 2 existen $c_s \in W(K)$ y $\varphi = \sum_{r_s=0}^{p-1} \{\varphi^p_{r_s} \; a_s^{r_s}\}$ con $\varphi_{r_s} \in K$ tales que

$$\text{(a)} \qquad b_s = \wp c_s + \frac{\partial \varphi}{\partial la_s} \quad (\text{mód. } TW).$$

Tanto b_s como $\dfrac{\partial\varphi}{\partial\, la_s}$ pertenecen a k (mód. TW), luego

$$\wp\, c_s \in k \quad (\text{mód. } TW)$$

y por ser K puramente inseparable sobre k, también

$$c_s \in k \quad (\text{mód. } TW)$$

luego en (a) podemos suponer $c_s \in w_o$.

Además $\varphi_{r_s} \in K$, luego

$$\varphi_{r_s} = \sum_{r_1,\ldots,r_{s-1}=0}^{p-1} \varphi_{r_1,\ldots,r_s}\, \xi_1^{r_1}\cdots\xi_{s-1}^{r_{s-1}}$$

con $\varphi_{r_1,\ldots,r_s} \in k.$

Sea

$$\varphi' = \sum_{r_1,\ldots,r_s=0}^{p-1} \left\{ \varphi^p_{r_1,\ldots,r_s}\; a_1^{r_1}\cdots a_s^{r_s} \right\}$$

y

$$b_i' = b_i - \wp\, c_s - \frac{\partial\varphi'}{\partial\, la_i} \qquad (i = 1,\ldots,s)$$

Puesto que

$$\frac{\partial\varphi}{\partial\, la_s} = \frac{\partial\varphi'}{\partial\, la_s} \quad (\text{mód. } TW),$$

resulta

$$b_s' = 0 \quad (\text{mód. } TW)$$

y teniendo en cuenta la proposición 1

$$\sum_{i=1}^{s-1} b_i'\, dl\xi_i = \sum_{i=1}^{s} b_i\, dl\xi_i = 0 \qquad (\text{mód. } w_o\, dW + \Pi(W\, dW))$$

luego por hipótesis de inducción existen $c_i' \in w_o$ y

$$\varphi'' = \sum_{r_1,\dots,r_{s-1}=0}^{p-1} \left\{\varphi''^{p}_{r_1,\dots,r_{s-1}}\, a_1^{r_1}\dots a_{s-1}^{r_{s-1}}\right\} \quad \text{con } \varphi''_{r_1,\dots,r_{s-1}} \in k$$

tales que

$$b_i' = \wp c_i' + \frac{\partial \varphi''}{\partial la_i} \qquad (\text{mód. } TW) \qquad (i = 1,\dots,s-1)$$

Poniendo

$$c_i = c_i' + c_s \qquad (i = 1,\dots,s-1)$$

$$f_{r_1,\dots,r_s} = \varphi_{r_1,\dots,r_s} \text{ si } r_s \neq 0,\; f_{r_1,\dots,r_{s-1},0} = \varphi''_{r_1,\dots,r_{s-1}}$$

$$f = \sum_{r_1,\dots,r_s=0}^{p-1} \left\{f^{p}_{r_1,\dots,r_s}\, a_1^{r_1}\dots a_s^{r_s}\right\}$$

y observando que

$$\frac{\partial f}{\partial la_i} = \frac{\partial \varphi'}{\partial la_i} + \frac{\partial \varphi''}{\partial la_i} \qquad (\text{mód. } TW) \qquad (i = 1,\dots,s-1)$$

$$\frac{\partial f}{\partial la_s} = \frac{\partial \varphi'}{\partial la_s} \qquad (\text{mód. } TW)$$

tenemos

$$b_i = \wp c_i + \frac{\partial f}{\partial la_i} \qquad (\text{mód. } TW) \quad (i = 1,\dots,s)$$

como se queria demostrar

<u>Proposición 3</u>.- Si $a_1,\dots,a_s$ son elementos p-independientes de k, $\xi_i^{p^n} = a_i$, $b_1,\dots,b_s$ vectores de w_o, y

$$\sum_{i=1}^{s} b_i \, dl\xi_i = 0 \quad (\text{mód. } w_o \, dW + \Pi(W \, dW)).$$

Entonces existen vectores $c_1,\dots,c_s$ de w_o y elementos $f_{r_1,\dots,r_s} \in k$ tales que

$$b_i = \wp c_i + \frac{\partial f}{\partial la_i} \quad (\text{mód. } TW) \quad (i = 1,\dots,s)$$

con

$$f = \sum_{r_1,\dots,r_s=0}^{p^n-1} \left\{ f^{p^n}_{r_1,\dots,r_s} \, a_1^{r_1}\dots a_s^{r_s} \right\}$$

Demostración. Sean $\eta_i = \xi_i^p$ y $K = k(\eta_1,\dots,\eta_s)$, entonces tenemos

$$\sum_{i=1}^{s} b_i \, dl\xi_i = 0 \quad (\text{mód. } W(K) \, dW + \Pi \, (WddW))$$

con $\xi_i^p = \eta_i$ p-independientes en K, luego, por la proposición 2, existen $c_i' \in W(K)$ y

$$\varphi = \sum_{r_1,\dots,r_s=0}^{p-1} \left\{ \varphi^p_{r_1,\dots,r_s} \, \eta_1^{r_1}\dots\eta_s^{r_s} \right\}$$

con $\varphi_{r_1,\dots,r_s} \in K$, tales que

$$b_i = \wp c_i + \frac{\partial \varphi}{\partial l\eta_i} \quad (\text{mód. } TW) \quad (i = 1,\dots,s)$$

Puesto que $b = Pb - \wp b$, se tiene :

$$b_i = P^{n-1}b_i - \wp(P^{n-2}b_i + \ldots + b_i) =$$

$$= \wp(P^{n-1}c_i' - P^{n-2}b_i - \ldots - b_i) + P^{n-1}\frac{\partial\varphi}{\partial l\eta_i} \quad (\text{mód.TW})$$

Ahora bien

$$P^{n-1}\frac{\partial\varphi}{\partial l\eta_i} = \sum_{r_1,\ldots,r_s=0}^{p-1} r_i \left\{\varphi^{p^n}_{r_1,\ldots,r_s} a_1^{r_1}\ldots a_s^{r_s}\right\}$$

con $\varphi_{r_1,\ldots,r_s} \in K$ luego

$$\varphi_{r_1,\ldots,r_s} = \sum_{t_1,\ldots,t_s=0}^{p^{n-1}-1} \varphi_{r_1,\ldots,r_s;t_1,\ldots,t_s}\eta_1^{t_1}\ldots\eta_s^{t_s}$$

con $\varphi_{r_1,\ldots,r_s;t_1,\ldots,t_s} \in k.$

Sea

$$f_{j_1,\ldots,j_s} = \sum_{r_i+pt_i=j_i} \varphi_{r_1,\ldots,r_s;t_1,\ldots,t_s}$$

y

$$f = \sum_{j_1,\ldots,j_s=0}^{p^n-1}\left\{f^{p^n}_{j_1,\ldots,j_s} a_1^{j_1}\ldots a_s^{j_s}\right\},$$

entonces módulo TW es

$$\frac{\partial f}{\partial l a_i} = \sum_{j_1,\ldots,j_s=0}^{p^n-1} j_i\left\{f^{p^n}_{j_1,\ldots,j_s} a_1^{j_1}\ldots a_s^{j_s}\right\} =$$

$$= \sum_{\substack{r_1,\ldots,r_s=0,\ldots,p-1\\ t_1,\ldots,t_s=0,\ldots,p^{n-1}-1}} (r_i + pt_i)\left\{\varphi^{p^n}_{r_1,\ldots,r_s;t_1,\ldots,t_s} a_1^{r_1+pt_1}\ldots a_s^{r_s+pt_s}\right\} =$$

$$= \sum_{\substack{r_1,\ldots,r_s=0,\ldots,p-1\\ t_1,\ldots,t_s=0,\ldots,p^{n-1}-1}} r_i\left\{\varphi^{p^n}_{r_1,\ldots,r_s;t_1,\ldots,t_s} a_1^{r_1+pt_1}\ldots a_s^{r_s+pt_s}\right\} =$$

$$= \sum_{r_1,\dots,r_s=0}^{p-1} r_i \left\{ \varphi_{r_1,\dots,r_s}^{p^n} a_1^{r_1}\cdots a_s^{r_s} \right\} = p^{n-1} \frac{\partial \varphi}{\partial l \xi_i}$$

luego

$$b_i = \wp c_i + \frac{\partial f}{\partial l a_i} \quad (\text{mód. } TW)$$

donde $c_i = p^{n-1} c_i' - p^{n-2} b_i - \dots - b_i \in w_o$.

Esta proposición 3 nos da la forma de la primera componente de b_i, y sirve de base para demostrar la siguiente proposición 4 que definitivamente nos proporciona la forma de las n primeras componentes de los vectores b_i.

Proposición 4 (teorema reciproco).- Si $a_1,\dots,a_s$ son elementos p-independientes de k, $\xi_i^{p^n} = a_i$, $b_1,\dots,b_s$ vectores de w_o, y

$$\sum_{i=1}^{s} b_i \, dl\xi_i = 0 \quad (\text{mód. } w_o \, dW + \pi(W \, dW))$$

Entonces existen vectores $c_1,\dots,c_s$ de w_o y elementos $f_{r_1,\dots,r_s} \in k$ tales que

$$b_i = \wp c_i + \frac{\partial f}{\partial l a_i} \quad (\text{mód. } T^n W) \quad (i = 1,\dots,s)$$

con

$$f = \sum_{r_1,\dots,r_s=0}^{p^n-1} \left\{ f_{r_1,\dots,r_s}^{p^n} a_1^{r_1}\cdots a_s^{r_s} \right\}$$

Demostración por inducción sobre n. Para $n = 1$ es la proposición 2. Supongamos la proposición cierta para $1,\ldots,n-1$.

Por la proposición 3 existen $c_i' \in W_o$ y

$$\varphi = \sum_{r_1,\ldots,r_s=0}^{p^n-1} \{\varphi^{p^n}_{r_1,\ldots,r_s} \; a_1^{r_1}\ldots a_s^{r_s}\}$$

con $\varphi_{r_1,\ldots,r_s} \in k$ tales que

$$b_i = \beta c_i' + \frac{\partial \varphi}{\partial l a_i} \quad (\text{mód. } TW) \quad (i = 1,\ldots,s)$$

o sea

$$b_i = \beta c_i' + \frac{\partial \varphi}{\partial l a_i} + T b_i' \qquad b_i' \in W_o$$

y pueden considerarse los términos de φ, cuyos índices son todos múltiplos de p, nulos, puesto que su contribución a $\frac{\partial \varphi}{\partial l a_i}$ módulo TW es nula, ya que ellos dan lugar a vectores múltiplos de p.

Teniendo en cuenta la proposición 1 resulta:

$$0 = \sum_{i=1}^{s} b_i \, dl\xi_i = \sum_{i=1}^{s} T b_i' \, dl\xi_i \quad (\text{mód. } W_o\, dW + \Pi(W\, dW))$$

pero módulo $\Pi(W\, dW)$ es

$$T b_i' \, dl\xi_i = (P^{-1} p b_i') \, dl\xi_i = b_i' \, dl\xi_i^{P}$$

llamando pues $\xi_i^{p} = \eta_i$ tenemos:

$$\sum_{i=1}^{s} b_i' \, dl \zeta_i = 0 \qquad (\text{mód. } w_o \, dW + \Pi \, (W \, dW))$$

y $\zeta_i^{p^{n-1}} = a_i$, luego,por hipótesis de inducción, existen $c_i'' \in w_o$ y $\varphi'_{r_1,\ldots,r_s} \in k$ tales que

$$b_i' = \beta c_i'' + \frac{\partial \varphi'}{\partial la_i} \quad (\text{mód. } T^{n-1}W)$$

con

$$\varphi' = \sum_{r_1,\ldots,r_s=0}^{p^{n-1}-1} \left\{ \varphi'^{\,p^{n-1}}_{r_1,\ldots,r_s} \, a_1^{r_1} \ldots a_s^{r_s} \right\}$$

luego

$$Tb_i' = \beta \, Tc_i'' + T \frac{\partial \varphi'}{\partial la_i} \qquad (\text{mód. } T^n W)$$

Además

$$Tb_i' = P^2 Tb_i' - \beta(PTb_i' + Tb_i') = \beta c_i''' + TP^2 \frac{\partial \varphi'}{\partial la_i} \quad (\text{mód. } T^n W)$$

donde se ha puesto

$$c_i''' = TP^2 c_i'' - PTb_i' - Tb_i'$$

Y teniendo en cuenta el teorema 2 del §1 tenemos:

$$TP^2 \frac{\partial \varphi'}{\partial la_i} = TP^2 \sum_{r_1,\ldots,r_s=0}^{p^{n-1}-1} r_i \left\{ \varphi'^{\,p^{n-1}}_{r_1,\ldots,r_s} \, a_1^{r_1} \ldots a_s^{r_s} \right\} =$$

$$= \sum_{r_1,\ldots,r_s=0}^{p^{n-1}-1} pr_i \left\{ \varphi'^{\,p^{n}}_{r_1,\ldots,r_s} \, a_1^{pr_1} \ldots a_s^{pr_s} \right\}$$

Poniendo pues

$f_{r_1,\ldots,r_s} = \varphi_{r_1,\ldots,r_s}$ si existe algún índice no divisible por p , $f_{pt_1,\ldots,pt_s} = \varphi'_{t_1,\ldots,t_s}$, $c_i = c_i' + c_i'''$

$$f = \sum_{r_1,\dots,r_s=0}^{p^n-1} \left\{ f^{p^n}_{r_1,\dots,r_s} \, a_1^{r_1}\cdots a_s^{r_s} \right\}$$

tenemos

$$b_i = \delta c_i + \frac{\partial f}{\partial la_i} \qquad (\text{mód. } T^n W)$$

con lo que queda demostrado el teorema.

§ 6. Demostración del teorema 3'.

Volvamos a las notaciones del §2.

En 1936 O.Teichmüller demostró el teorema en los casos particulares $n = 1$ ([4] teorema 26) y $s = 1$ ([5]), apoyándose en el siguiente teorema de E. Witt

[4] teorema 7.- Si $a \notin k^p$, $(a|b]_1 = k[u,v]$, $y = c_0 + \dots + c_{p-1}u^{p-1} \in k(u)$. Entonces se verifica

$$\wp(y + v) = y^p - c_0 + \wp v = y^p - c_0 + b$$

En este § vamos a demostrar el teorema para n y s cualesquiera, independientemente del módulo de formas de Pfaff introducido en el § 3

Proposición 1'(teorema directo) .- Si los vectores $b_1,\dots,b_s$ son de la forma

$$b_i = \wp c_i + \frac{\partial f}{\partial la_i} \quad (\text{mód. } T^n W) \qquad (i = 1,\dots,s)$$

con $a_1,\dots,a_s$ p-independientes en k, $f_{r_1,\dots,r_s} \in k$, $c_i \in W_0$ y

$$f = \sum_{r_1,\dots,r_s=0}^{p^n-1} \{f^{p^n}_{r_1,\dots,r_s} a_1^{r_1}\dots a_s^{r_s}\}$$

entonces es

$$\sum_{i=1}^{s} (a_i|b_i]_n = 0$$

Demostración. Por la linealidad en b basta demostrar:

a) $(a_i | \wp c_i]_n = 0$ y b) $\sum_{i=1}^{s} (a_i | \frac{\partial f}{\partial la_i}]_n = 0$

a) es consecuencia inmediata de (4) del § 2:

$$(a_i | \wp c_i]_n = (a_i | Fc_i]_n - (a_i | c_i]_n = 0$$

b) Por (1) y (2) del § 2 tenemos:

$$\sum_{i=1}^{s} (a_i | \frac{\partial f}{\partial la_i}]_n = \sum_{\substack{i=1,\dots,s \\ r_1,\dots,r_s=0,\dots,p^n-1}} (a_i | r_i \{ f^{p^n}_{r_1,\dots,r_s} a_1^{r_1}\dots a_s^{r_s}\}]_n =$$

$$= \sum_{\substack{i=1,\dots,s \\ r_1,\dots,r_s=0,\dots,p^n-1}} (a_i^{r_i} | \{ f^{p^n}_{r_1,\dots,r_s} a_1^{r_1}\dots a_s^{r_s}\}]_n =$$

$$= \sum_{r_1,\dots,r_s=0,\dots,p^n-1} (a_1^{r_1}\dots a_s^{r_s} | \{ f^{p^n}_{r_1,\dots,r_s} a_1^{r_1}\dots a_s^{r_s}\}]_n$$

que por (5) del § 2 es nulo.

<u>Proposición 2'</u>(teorema recíproco para $n = 1$).- Si $a_1,\dots,a_s$ son p-independientes en k, $b_1,\dots,b_s$ vectores de w_o y

$$(a_i | b_i]_1 = 0$$

entonces existen vectores $c_1,\dots,c_s$ de w_o y elementos $f_{r_1,\dots,r_s} \in k$ tales que

$$b_i = \wp c_i + \frac{\partial f}{\partial la_i} \qquad (\text{mód. } TW)$$

con

$$f = \sum_{r_1,\dots,r_s=0}^{p-1} \{ f^p_{r_1,\dots r_s} \, a_1^{r_1}\dots a_s^{r_s} \}$$

Demòstrado en teorema 26.

<u>Proposición 3</u>'.- Si $a_1,\dots,a_s$ son elementos p-independientes de k, $b_1,\dots,b_s$ vectores de w_o y

$$\sum_{i=1}^{s} (a_i | b_i]_n = 0.$$

Entonces existen vectores $c_1,\dots,c_s$ de w_o y elementos $f_{r_1,\dots,r_s} \in k$ tales que

$$b_i = \wp c_i + \frac{\partial f}{\partial la_i} \qquad (\text{mód. } TW)$$

con

$$f = \sum_{r_1,\dots,r_s=0}^{p^n-1} \{ f^{p^n}_{r_1,\dots,r_s} \, a_1^{r_1}\dots a_s^{r_s} \} .$$

Demostración. Sean

$$(a_i | b_i]_n = k[u_i ; v_{i,o},\dots,v_{i,n-1}]$$

con las relaciones

$$u_i^{p^n} = a_i, \ \wp v_i = b_i, \ u_i v_i u_i^{-1} = v_i + \{1\}$$

donde v_i indica el vector $(v_{i,o},\dots,v_{i,n-1})$ (vid. §2) y

$$(a_i | 0]_n = k[u_i' ; v_{i,o}',\dots,v_{i,n-1}']$$

con las relaciones

$$u_i'^{p^n} = a_i, \quad \wp v_i' = 0, \quad u_i' v_i' u_i'^{-1} = v_i' + \{1\}.$$

Por hipótesis es

$$\sum_{i=1}^{s} (a_i | b_i]_n = 0$$

es decir el álgebra

$$A = \prod_{i=1}^{s} (a_i | b_i]_n$$

producto directo de las álgebras $(a_i | b_i]_n$ es un álgebra total de matrices de grado p^{ns} , luego es isomorfa al álgebra

$$A' = \prod_{i=1}^{s} (a_i | 0]_n .$$

Puesto que $a_1, \ldots, a_s$ son p-independientes, las subálgebras

$$k[u_1, \ldots, u_s] \cong k[u_1', \ldots, u_s']$$

son subcuerpos isomorfos de A y A' y el isomorfismo $A \cong A'$ puede considerarse prolongación del isomorfismo entre aquellos subcuerpos (*), y las álgebras A y A' como una misma álgebra con $u_i = u_i'$:

$$k[u_1, \ldots, u_s; v_1, \ldots, v_s] = k[u_1, \ldots, u_s; v_1', \ldots, v_s']$$

donde

$$v_i = (v_{i,o}, \ldots, v_{i,n-1}) \ , \quad v_i' = (v_{i,o}', \ldots, v_{i,n-1}') \quad (i=1,\ldots,s)$$

(*) A. Albert th. 4. 14.

En esta álgebra tenemos:

$$u_i(v_{i,o} - v'_{i,o})u_i^{-1} = v_{i,o} - v'_{i,o}$$

luego $y_i = v_{i,o} - v'_{i,o}$ es permutable con todas las u

y por tanto

$$y_i \in k[u_1,\ldots,u_s]$$

ya que este cuerpo es maximal conmutativo en A (*)

Sea pues

$$y_i = \sum_{r_1,\ldots r_s=0}^{p^n-1} c_{r_1,\ldots,r_s;i}\, u_1^{r_1}\ldots u_s^{r_s} \qquad (i = 1,\ldots,s)$$

con $c_{r_1,\ldots,r_s;i} \in k.$

El álgebra

$$k[u_1,\ldots,u_s,v'_{i,o}]$$

puede considerarse como el álgebra $(u_i^p|0]_1$ sobre su centro

$$k[u_1,\ldots,u_{i-1},u_i^p,u_{i+1},\ldots,u_s]$$

La primera componente de b_i viene dada por

$$b_{i,o} = \int v_{i,o} = \int(y_i + v'_{i,o})$$

y por [4] teorema 7 aplicado al álgebra $(u_i^p|0]_1$ anteriormente considerada es

---

(*) A: Albert th. 4. 12.

$$b_{i,o} = y_i^p - c_{i,o}$$

donde $c_{i,o}$ es el término independiente de la expresión de y_i como polinomio en u_i con coeficientes del cuerpo

$$k\left[u_1,\dots,u_{i-1},u_i^p,u_{i+1},\dots,u_s\right]$$

es decir

$$c_{i,o} = \sum_{p\mid r_i} c_{r_1,\dots,r_s;i}\, u_1^{r_1}\dots u_s^{r_s}$$

donde los índices del sumatorio toman todos los valores de 0 a p^n-1, salvo el índice r_i que sólo toma valores múltiplos de p. También puede ponerse

$$b_{i,o} = \wp\, y_i + \sum_{p\nmid r_i} c_{r_1,\dots,r_s;i}\, u_1^{r_1}\dots u_s^{r_s}$$

donde los índices del sumatorio toman todos los valores de 0 a p^n-1 salvo el índice r_i que sólo toma valores no múltiplos de p.

Teniendo en cuenta

$$b_{i,o} = P^n b_{i,o} - \wp(P^{n-1}b_{i,o}+\dots+ b_{i,o})$$

y sustituyendo en $P^n b_{i,o}$, $b_{i,o}$ por la expresión antes hallada se tiene

$$b_{i,o} = \wp\, c_i + \sum_{p\nmid r_i} c^{p^n}_{r_1,\dots,r_s;i}\, a_1^{r_1}\dots a_s^{r_s}$$

donde se ha puesto

$$c_i = P^n y_i - P^{n-1} b_{i,o} - \ldots - b_{i,o} \in k$$

Para que esta expresión de $b_{i,o}$ sea de la forma deseada tenemos que probar que los coeficientes

$$r_i^{-1} \; c_{r_1,\ldots,r_s;i}$$

no dependen del índice i. Para ello consideremos los productos

$$v_{j,o} v_{i,o} = (v'_{j,o} + y_j)(v'_{i,o} + y_i) =$$

$$= v'_{j,o} v'_{i,o} + v'_{j,o} y_i + y_j v'_{i,o} + y_j y_i$$

$$v_{i,o} v_{j,o} = (v'_{i,o} + y_i)(v'_{j,o} + y_j) =$$

$$= v'_{i,o} v'_{j,o} + v'_{i,o} y_j + y_i v'_{j,o} + y_i y_j$$

y puesto que

$$v_{j,o} v_{i,o} = v_{i,o} v_{j,o} \,, \; v'_{j,o} v'_{i,o} = v'_{i,o} v'_{j,o} \,, \; y_j y_i = y_i y_j$$

resulta

$$v'_{j,o} y_i + y_j v'_{i,o} = v'_{i,o} y_j + v'_{j,o} y_i$$

Teniendo ahora en cuenta la regla de commutación de las u con las v tenemos

$$y_j v'_{i,o} = \sum_{r_1,\dots,r_s=0}^{p^n-1} c_{r_1,\dots,r_s;j}\, u_1^{r_1}\cdots u_s^{r_s}\, v'_{i,o} =$$

$$= \sum_{r_1,\dots,r_s=0}^{p^n-1} r_i c_{r_1,\dots,r_s;j}\, u_1^{r_1}\cdots u_s^{r_s} + v'_{i,o}\, y_j$$

$$y_i v'_{j,o} = \sum_{r_1,\dots,r_s=0}^{p^n-1} r_j c_{r_1,\dots,r_s;i}\, u_1^{r_1}\cdots u_s^{r_s} + v'_{j,o}\, y_i$$

luego

$$\sum_{r_1,\dots,r_s=0}^{p^n-1} r_i c_{r_1,\dots,r_s;j}\, u_1^{r_1}\cdots u_s^{r_s} = \sum_{r_1,\dots,r_s=0}^{p^n-1} r_j c_{r_1,\dots,r_s;i}\, u_1^{r_1}\cdots u_s^{r_s}$$

y por tanto

$$r_i c_{r_1,\dots,r_s;j} = r_j c_{r_1,\dots,r_s;i}$$

es decir los cocientes

$$r_i^{-1} c_{r_1,\dots,r_s;i}$$

no dependen de i y podemos definir

$$f_{r_1,\dots,r_s} = r_i^{-1} c_{r_1,\dots,r_s;i} \qquad \text{si } p \nmid r_i$$

con lo que resulta

$$b_{i,o} = \delta c_i + \sum_{p \nmid r_i} r_i\, f^{p^n}_{r_1,\dots,r_s}\, a_1^{r_1}\cdots a_s^{r_s}$$

Pero si $p \mid r_i$, es $r_i = 0$ en k, luego

$$b_{i,o} = \rho c_i + \sum_{r_1,\dots r_s=0}^{p^n-1} r_i f^{p^n}_{r_1,\dots,r_s} a_1^{r_1}\dots a_s^{r_s}$$

como se quería demostrar.

Nótese que si p divide a todos los índices, entonces $f_{pt_1,\dots,pt_s}$ no está definido, pero sea cual sea el valor que se le atribuya su contribución a la primera componente de cualquier b_i es nula.

<u>Proposición 4'</u>(teorema recíproco).- Si $a_1,\dots,a_s$ son elementos p-independientes de k, $b_1,\dots,b_s$ vectores de W_o y

$$\sum_{i=1}^{s} (a_i | b_i]_n = 0.$$

Entonces existen vectores $c_1,\dots,c_s$ de W_o y elementos $f_{r_1,\dots,r_s} \in k$ tales que

$$b_i = \rho c_i + \frac{\partial f}{\partial la_i} \qquad (\text{mód. } T^n W)$$

con

$$f = \sum_{r_1,\dots r_s=0}^{p^n-1} \{ f^{p^n}_{r_1,\dots,r_s} a_1^{r_1}\dots a_s^{r_s} \}$$

Demostración por inducción sobre n. Para $n = 1$ es la proposición 2'. Por la proposición 3' existen

$$c_i' \in W_o \qquad y \qquad \varphi = \sum_{r_1,\dots r_s=0}^{p^n-1} \{ \varphi^{p^n}_{r_1,\dots,r_s} a_1^{r_1}\dots a_s^{r_s} \}$$

con $\varphi_{r_1,\ldots,r_s} \in k$ tales que

$$b_i = \wp c'_i + \frac{\partial \varphi}{\partial la_i} + Tb'_i \qquad b'_i \in W_o$$

Por la proposición 1' es

$$\sum_{i=1}^{s} (a_i | \wp c'_i + \frac{\partial \varphi}{\partial la_i}]_n = 0$$

luego

$$0 = \sum_{i=1}^{s} (a_i | b_i]_n = \sum_{i=1}^{s} (a_i | Tb'_i]_n$$

o sea por (4) del § 2

$$\sum_{i=1}^{s} (a_i | b'_i]_{n-1} = 0$$

luego por hipótesis de inducción existen

$$c''_i \in W_o \qquad y \qquad \varphi' = \sum_{r_1,\ldots,r_s=0}^{p^{n-1}-1} \{\varphi'_{r_1,\ldots,r_s}{}^{p^{n-1}} a_1^{r_1}\ldots a_s^{r_s}\}$$

con $\varphi'_{r_1,\ldots,r_s} \in k$ tales que

$$b'_i = \wp c''_i + \frac{\partial \varphi'}{\partial la_i} \qquad (\text{mód. } T^{n-1}W)$$

luego

$$Tb'_i = \wp Tc''_i + T\frac{\partial \varphi'}{\partial la_i} \qquad (\text{mód. } T^n W)$$

y se termina la demostración como en la proposición 4 del §5.

BIBLIOGRAFIA

[1] A.A. Albert. Structure of algebras. Am. Math. Soc. Publ. XXIV (1939)

[2] R. Brauer. Untersuchungen über die aritmetische Eigenschaften von Gruppen linearer Substitutionen. I Y II Math. Zeitsch. 28 (1928) y 31 (1930)

[3] E. Kähler. Ueber rein algebraische Körper. Math. Nachr. 5 (1951)

[4] O. Teichmüller. p-Algebren. Deutsche Mathematik 1 (1936)

[5] O. Teichmüller. Zerfallende zyclische p-Algebren. Crelle 176 (1936)

[6] J.H.M. Wedderburn. On hypercomplex numbers. Proc. London Math. Soc. 6 (1907)

[7] E. Witt. Zyclische Körper und Algebren der Charakteristik p vom Grad p^n. Struktur diskret bewerteter Körper mit vollkommenem Restklassen Körper der Charakteristik p. Crelle 176 (1936).

[8] E. Witt. p-Algebren und Pfaffschen Formen. Abh. Math. Sem. Hamburg 22 (1958).