UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS BASICAS Y FARMACEUTICAS
DEPARTAMENTO DE MATEMATICAS

DISCRIMINANTES EN CARACTERISTICA 2.

Tesis para optar al Grado
de Licenciado en Ciencias
con mención en Matemáticas

Prof. Guía Dr. R. Baeza

MARIA INES ICAZA PEREZ

1983

A mis padres.

I N D I C E.

INTRODUCCION.

En el trabajo "An Analog to the Discriminant over fields of Characteristic two", E.R. Berlekamp introduce una nueva invariante para extensiones finitas y separables, L/F donde F es un cuerpo de característica 2. Esta invariante que se define a partir del polinomio que genera la extensión, resulta tener la propiedad galoisiana de la discriminante de extensiones finitas y separables definida para el caso en que la característica de F es distinta de dos, es decir, si $F \subseteq L$, L finita y separable, car $F \neq 2$ $L = F(\theta)$ y $G = Gal(N/F)$ donde N es cerradura normal de L/F, entonces considerando $G \hookrightarrow S_n$, S_n el grupo simétrico, la discriminante de L/F, $\Delta_{L/F}$ tiene la propiedad galoisiana siguiente $F(\sqrt{\Delta_{L/F}}) = Fix(G \cap An)$ donde An denota al grupo alternante, la cual en el caso $2 = 0$ se cumple para la invariante de Berlekamp, es decir, esta invariante es un análogo de la discriminante usual para el caso $2 = 0$.

En su trabajo, Berlekamp solo introduce esta discriminante. Nuestro propósito es estudiar la discriminante de Berlekamp, encontrar propiedades análogas a las de la discriminante usual y aplicarlas en algunos resultados, especialmente en los obtenidos por A. Wadsworth en su trabajo "Discriminants

in characteristic 2", que servirá para calcular la discriminante de Berlekamp del trinomio $ax^n + bx^k + c$ sobre un cuerpo de característica 2 (Teorema (4.3)) y luego para determinar la paridad de la cantidad de factores irreducibles que se obtienen al descomponer este trinomio sobre $GF(2^m)$ (Teorema (4.8)) con lo que obtendremos una generalización del corolario de Swan-Berlekamp que sólo trata el caso $x^n + x^k + 1$ sobre $GF(2)$. En la segunda parte, aplicaremos los resultados de Wadsworth para dar una demostración más simple en el caso de automorfismos propios, del Teorema (1.2) del trabajo "Discriminants of Polynomials and Quadratic Forms" de R. Baeza, utilizando la demostración dada por B. Edwards para el caso $2 \neq 0$. Finalmente, en el Apéndice, definiremos otra discriminante, introducida por Revoy en "Remarques sur la forme trace" y daremos la demostración de A. Wadsworth de la conjetura de Revoy que relaciona ambas discriminantes definidas en el caso $2 = 0$.

El trabajo se desarrolla como sigue:

En el Capítulo I, párrafo 1, definimos desde el punto de vista galoisiano la discriminante usual, para el caso $2 \neq 0$ y la de Berlekamp para el caso $2 = 0$. En el segundo párrafo se demuestran propiedades de la discriminante de Berlekamp y se define la resultante de dos polinomios, como análoga a la resultante en el caso $2 \neq 0$. En el pá-

rrafo 3 se introducen los resultados de A. Wadsworth que se utilizan en el párrafo 4, para determinar la paridad de factores que descomponen el trinomio $ax^n + bx^k + c$ sobre un cuerpo de característica 2.

En el Capítulo 2, párrafo 1 se introducen algunas nociones básicas de la teoría de formas cuadráticas sobre anillos semi-locales y se relaciona la discriminante de Berlekamp con formas cuadráticas, y en el párrafo 2 se dá una demostración más simple del teorema fundamental del trabajo "Discriminants of Polynomials and of Quadratics Forms" de R. Baeza. En el Apéndice se introduce una nueva discriminante para el caso $2 = 0$, definido por Revoy y se demuestra la relación con la discriminante de Berlekamp.

Agradezco al Dr. Ricardo Baeza el haberme permitido desarrollar este tema bajo su dirección.

CAPITULO I. DISCRIMINANTES DE POLINOMIOS.

§ 1. Definiciones generales.

El propósito de este párrafo es dar una definición desde el punto de vista galoisiano de la discriminante de un polinomio separable sobre un cuerpo F que en el caso de $\operatorname{car} F \neq 2$ conduce a la definición usual de discriminante y en el caso $\operatorname{car} F = 2$ se reduce a la discriminante definida por Berlekamp en $[Be]_2$. La ventaja de este punto de vista es la posibilidad de generalizar el concepto de discriminante a polinomios con coeficientes en un anillo cualquiera.

Sea F cuerpo cualquiera. Sea $f(x) \in F[x]$ un polinomio separable y consideremos un cuerpo de descomposición de $f(x)$ sobre F. Sea $L = F(\alpha_1, \ldots, \alpha_n)$ con $f(x) = a(x - \alpha_1) \ldots (x - \alpha_n)$, $a \in F^*$.
La extensión L/F es galoisiana y denotaremos por G el grupo de Galois de L/F. Se sabe que existe una inclusión $G \hookrightarrow S_n$ el grupo de permutaciones de n elementos.
Sea $A_n \lhd S_n$ el subgrupo alternante y $H = G \cap A_n$. En general se tiene $[G : H] \leq 2$ pudiendo suceder el caso $G = H$ (Ver 1.1. más abajo). Sea $K = \operatorname{Fix}(H)$ tenemos entonces $F \subseteq K \subseteq L$ y $[K : F] \leq 2$. La extensión K/F es una extensión separable.

(1.1.) Definición: La discriminante de $f(x)$ sobre F es la extensión K/F . Diremos que la discriminante de $f(x)$ es trivial si $K = F$ es decir $G = H$. En el otro caso $[K : F] = 2$ y a continuación, en este caso, describiremos la extensión K explícitamente. Para esto consideremos los casos car $F \neq 2$ y car $F = 2$ separadamente.

i) Car $F \neq 2$.

Consideremos el elemento:

$$\delta = \prod_{i<j} (\alpha_i - \alpha_j) \in \tilde{L}$$

Entonces $\Delta := \delta^2 = \prod_{i<j} (\alpha_i - \alpha_j)^2 \in F$ pués G deja fijo a δ^2 . Por otro lado como $H < A_n$ se tiene que H deja invariante al elemento δ y luego $\delta \in K$. Tenemos entonces las siguientes equivalencias:

(1.2.) Proposición: 1) $\delta \notin F$ si y sólo si $[K : F] = 2$ y en este caso $K = F(\delta) = F(\sqrt{\Delta})$

2) $\delta \in F$ si y sólo si $K = F$. En este caso $\Delta \in F^{*2}$.

Demostración: 1) Se tiene $2 \leq [F(\delta) : F] \leq [K : F] \leq 2$.

Luego tenemos $\delta \notin F$ implica $[K : F] = 2$.

Ahora resulta fácil demostrar:

Si $\sigma \in G \hookrightarrow S_n$, entonces $\sigma(\delta) = (\text{sign } \sigma) \cdot \delta$

Luego si $[K : F] = 2$ entonces existe $\sigma \in G$, $\sigma \notin H$ pero $\sigma(\delta) = (\text{sign}\sigma).\delta \neq \delta$ pués σ es impar, luego se tiene $\delta \notin F$. Por lo tanto tenemos $\delta \notin F$ si y sólo si $[K : F] = 2$. En este caso como $F(\delta) \subseteq K$ se tiene $F(\delta) = K$.

2) Inmediato por (1).

Por la proposición anterior, la clase $\bar{\Delta} \in F^*/F^{*2}$ caracteriza la extensión K/F y coincide con la discriminante usual de un polinomio. En el futuro, si car $F \neq 2$ identificaremos la discriminante de un polinomio $f(x) = a \prod_{i=1}^{n} (x - \alpha_i)$, con la clase de $\Delta = \prod_{i<j} (\alpha_i - \alpha_j)^2$ en $F^*/_{F^{*2}}$.

En la literatura también se denota por la discriminante de F al elemento $a^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2 \in F^*$ (el coeficiente a^{2n-2} es un cuadrado, luego no altera la clase en F^*/F^{*2}).

ii) Sea car $F = 2$.

Para caracterizar la extensión K/F, se introduce el grupo $F/p(F)$ donde $p(F) = \{x^2 + x / x \in F\}$. Los elementos de $F/p(F)$ están en correspondencia biunívoca con las clases de isomorfía de extensiones cuadráticas separables. Concretamente, a la clase $\bar{a} \in F/p(F)$ le corresponde la extensión $F(p^{-1}(a))$, donde $p^{-1}(a)$ es una raíz del polinomio $x^2 + x + a$.

Consideremos ahora los elementos:

$$\beta = \sum_{i<j} \frac{\alpha_i}{\alpha_i + \alpha_j} \in L$$

$$D(f) = \sum_{i<j} \frac{\alpha_i \alpha_j}{\alpha_i^2 + \alpha_j^2} \in F$$

Entonces $p^{-1}(D(f)) = \beta$ pués se tiene:

$$\left(\sum_{i<j} \frac{\alpha_i}{\alpha_i + \alpha_j} \right)^2 + \sum_{i<j} \frac{\alpha_i}{\alpha_i + \alpha_j} + \sum_{i<j} \frac{\alpha_i \alpha_j}{\alpha_i^2 + \alpha_j^2} =$$

$$= \sum_{i<j} \left(\frac{\alpha_i^2}{\alpha_i^2 + \alpha_j^2} + \frac{\alpha_i^2 + \alpha_i \alpha_j}{\alpha_i^2 + \alpha_j^2} + \frac{\alpha_i \alpha_j}{\alpha_i^2 + \alpha_j^2} \right) = 0$$

Se tiene además $D(f) \in F$ ya que queda fijo bajo la acción de G.

Además H deja invariante al elemento $p^{-1}(D(f)) = \beta$. Luego $\beta \in K$ y nuevamente se tienen las equivalencias:

(1.3) Proposición: 1) $\beta \notin F$ sí y sólo sí $[K : F] = 2$. En este caso $K = F(\beta) = F(p^{-1}(D(f))$.

2) $\beta \in F$ si y sólo si $K = F$. En este caso $D(f) \in p(F)$.

Demostración: 1) $\beta \notin F$ si y sólo si $[F(\beta) : F] \geq 2$. Pero $2 \leq [F(\beta) : F] \leq [K : F] \leq 2$ luego $[K : F] = 2$.

Además se tiene nuevamente, dado $\sigma \in G \hookrightarrow S_n$, $\sigma(\beta) = \beta + \frac{1 - \text{sign}\sigma}{2}$. Luego si $[K : F] = 2$ existe $\sigma \in G$,

$\sigma \notin H$ y tenemos $\sigma(\beta) = \beta + 1$, luego $\beta \notin F$. En este caso como $F(\beta) \subseteq K$, se tiene $F(\beta) = K$.

2) Inmediato por (1).

Análogamente al caso car $F \neq 2$ la clase $\overline{D(f)} \in F/\wp(F)$ caracteriza la extensión K/F y corresponde a la definición dada por Berlekamp en $[Be]_2$ para la discriminante de un polinomio sobre un cuerpo de característica 2. De la misma manera identificaremos la discriminante de un polinomio $f(x) = a \prod_{i=1}^{n} (x - \alpha_i)$ con la clase

$$\overline{D(f)} = \sum_{i<j} \frac{\overline{\alpha_i \alpha_j}}{\alpha_i^2 + \alpha_j^2} \in F/\wp(F)$$

Ejemplos: i) Sea $f(x) = x^2 + bx + c \in F[x]$ separable

(a) Si car $F \neq 2$ $\Delta(f) = b^2 - 4c$

(b) Si car $F = 2$ $D(f) = c/b^2$ ($b \neq 0$ pues f es separable).

ii) $f(x) = x^3 + bx^2 + cx + d \in F[x]$ separable.

(a) car $F \neq 2$ $\Delta(f) = (bc)^2 - 4c^3 - 4b^3d - 27d^2 + 18bcd$

(b) car $F = 2$ $D(f) = \dfrac{c^3 + cb + d}{(bc)^2 - d^2}$

En particular si

iii) $f(x) = x^3 + bx + c \in F[x]$ polinomio separable

(a) car $F \neq 2$ $\Delta(f) = -4b^3 - 27\,c^2$

(b) car $F = 2$ $\qquad D(f) = \dfrac{b^3 + bc + c}{c^2}$

Observación: En el caso car $F = 2$, se puede introducir la discriminante de $f(x)$, e.d. $D(f(x)) = \prod_{i<j} (\alpha_i - \alpha_j)^2$. Sólo que en este caso, la extensión cuadrática que se obtiene $L = F(\delta)$ con $\delta^2 = \Delta(f)$ es puramente inseparable.

Sean $F \subset L$ cuerpos, L extensión finita y separable $L = F(\theta)$, θ elemento primitivo y $f(x) \in F[x]$ polinomio minimal de θ . Podemos, entonces, generalizar la definición de discriminante de la extensión L/F a través de la discriminante del polinomio minimal de θ de la siguiente manera:

(i) Supongamos car $F \neq 2$. Entonces la discriminante de L/F : $\Delta_{L/F} := \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2 \pmod{F^{*2}}$ que es la discriminante de $f(x)$ con raíces $\theta = \theta_1, \ldots, \theta_r$ en alguna clausura algebraica de F .

(ii) Supongamos car $F = 2$. Entonces la discriminante de L/F es nuevamente la discriminante de $f(x)$, e.d.

$$D_{L/F} := \sum_{i<j} \frac{\theta_i \theta_j}{\theta_i^2 + \theta_j^2} \bmod p(F)$$

Observación: Existe también una definición dada por Revoy para la discriminante de L/F donde car $F = 2$. Ver apéndice.

Para el caso car $F \neq 2$, bajo las hipótesis anteriores, existe una relación entre la discriminante de L/F , $\Delta_{L/F}$ y la derivada del polinomio que genera la extensión $f(x)$.

(1.4) Proposición: Sea L/F extensión finita y separable, $L = F(\theta)$ con $[L : F] = n$ y $f(x)$ el polinomio minimal de θ sobre F . Entonces:

$$\Delta_{L/F} = N_{L/F}(f'(\theta)) \cdot (-1)^{\frac{n(n-1)}{2}}$$

Demostración: Sea $\bar{F}$ clausura algebraica de F y $\sigma_1(\theta), \ldots, \sigma_n(\theta)$ los distintos conjugados de θ en $\bar{F}$. Entonces $1, \theta, \ldots, \theta^{n-1}$ es base de L/F y

$$\Delta_{L/F} = \begin{vmatrix} 1 & \sigma_1 & \ldots\ldots & (\theta^{n-1})^{\sigma_1} \\ \vdots & & & \vdots \\ 1 & \sigma_n & \ldots\ldots & (\theta^{n-1})^{\sigma_n} \end{vmatrix}^2 = \pm \prod_{i \neq j} (\sigma_i(\theta) - \sigma_j(\theta))$$

Pués es el cuadrado de un determinante de Vandermonde.

Luego: $$\Delta_{L/F}(1, \theta, \ldots, \theta^{n-1}) = \prod_{i \neq j} (\sigma_i(\theta) - \sigma_j(\theta))$$

Por otro lado se tiene:

$$f(x) = \prod_{i=1}^{n} (x - \sigma_i(\theta))$$

y fijando σ_1 como la identidad, se verifica:

$$f'(\theta) = \prod_{i=2}^{n} (\theta - \sigma_i(\theta))$$

Luego
$$N_{L/F}(f'(\theta)) = \prod_{j=1}^{n} \sigma_j \prod_{i=2}^{n} (\theta - \sigma_i(\theta))$$

$$= \prod_{\substack{1\leq j\leq n \\ 2\leq i\leq n}} (\sigma_j(\theta) - \sigma_j\sigma_i(\theta))$$

Si fijamos j, entonces $\sigma_i\sigma_j$ recorre todas las conjugaciones excepto σ_j, cuando i recorre de 2 a n. Luego se tiene

$$N_{L/F}(f'(\theta)) = \prod_{i\neq j} (\sigma_j(\theta) - \sigma_i(\theta)) = \Delta_{L/F}\,(-1)^{\frac{n(n-1)}{2}}$$

En el caso en que car F = 2 no tenemos una fórmula análoga. Debido a la aditividad de la discriminante (ver § 2) se esperaría que la traza de la extensión L/F sirviera para expresar la discriminante $D_{L/F}$. Los ejemplos calculados comprueban esta afirmación pero no hemos podido encontrar una fórmula como en el caso $2 \neq 0$.

Para finalizar este párrafo daremos un criterio galoisiano para determinar la trivialidad de la discriminante de una extensión galoisiana L/F. (Ver [CP]).

(1.5) Teorema: Sea L/F extensión galoisiana finita con grupo de Galois G, $\#G = n$. Entonces:

$D_{L/F}$ es trivial si y sólo si $G \subseteq A_n$ si y sólo si G no contiene un 2-subgrupo de Sylow cíclico no trivial.

Demostración: $\Rightarrow$)

Consideremos la sucesión exacta:

$$0 \longrightarrow A_n \longrightarrow S_n \xrightarrow{\text{Sign}} \mathbb{Z}/_{2\mathbb{Z}} \longrightarrow 0$$

Sea $\sigma \in G$ y consideremos la representación regular de σ como permutación. Entonces:

(i) Supongamos que el orden de σ es impar. Luego existe $d \in \mathbb{Z}$ con

$$\sigma^d = \sigma^{2k}\sigma = 1\!\!1 \quad \text{luego} \quad \text{sign}\sigma = \text{sign}\, 1\!\!1$$

y se tiene $\sigma \in A_n$.

(ii) Supongamos que el orden de σ es par. Entonces existe $d \in \mathbb{Z}$ con:

$$\sigma^d = 1\!\!1 \quad , \quad d = 2^j \cdot m \quad ; \quad m \equiv 1 (\text{mod } 2)$$

Pero G opera transitivamente e.d. dados α_i, α_j raíces de $f(x)$, el polinomio que genera la extensión, existe $\delta \in G$ tal que $\delta(\alpha_i) = \alpha_j$.

Luego G no deja ningún punto fijo.

Ahora sea $\sigma = \sigma_1, \ldots, \sigma_r$ descomposición de σ en ciclos disjuntos. Entonces se tiene $ord(\sigma_i) \mid d$ y más aún $ord(\sigma_i) = d$ para todo i pues supongamos $ord(\sigma_j) < d$ para algún j, entonces σ^d dejaría fijo a los elementos del ciclo σ_j. Por lo tanto $ord(\sigma_j) = d$ para todo $j = 1, \ldots, r$.

Como $ord(\sigma_j) = \ell(\sigma_j)$. Se tiene que en la descomposición de σ como producto de ciclos disjuntos, todos los ciclos tienen largo d y como $\#G = n$, σ se descompone en $\frac{n}{d}$ ciclos disjuntos de largo d.

Como un ciclo de largo par proviene de una permutación impar, se tiene:

σ es par si y sólo si $\frac{n}{d}$ es par si y sólo si $\frac{n}{2^j m}$ es par si y sólo si 2^j es menor que la potencia máxima de 2 que divide a n.

Por lo tanto G no contiene 2-subgrupos de Sylow <u>cíclicos</u> no triviales.

$\Leftarrow$) Inmediata por las equivalencias anteriores.

<u>Nota</u>: En este teorema, $D_{L/F}$ denota la discriminante usual si $car\ F \neq 2$ y a la discriminante de Berlekamp si $car\ F = 2$ ya que la demostración en ambos casos es idéntica.

§ 2. Propiedades de la discriminante.

En este párrafo se estudiarán las propiedades de la discriminante usual, en el caso F cuerpo de característica $\neq 2$ y de la discriminante de Berlekamp en el caso car $F = 2$.

Se introducirá además la resultante de dos polinomios que en ambos casos aparece relacionada con la discriminante del producto de los polinomios y se estudiarán también sus propiedades.

Sea F cuerpos cualquiera, sea $f(x) \in F[x]$ polinomio separable y $K = F(\alpha_1, \ldots, \alpha_n)$ un cuerpo de descomposición de $f(x)$ sobre F . Sobre F se tiene $f(x) = a \prod_{i=1}^{n} (x - \alpha_i)$ $a \in F^*$.

Hagamos, nuevamente, la distinción entre los casos:

(i) car $F \neq 2$.

(2.1) Definición: Sea $g(x)$ polinomio separable sobre F y $L = F(\beta_1, \ldots, \beta_m)$ un cuerpo de descomposición de $g(x)$ sobre F .

$$g(x) = b \prod_{i=1}^{m} (x - \beta_i)$$

Se define la resultante de $f(x)$ y $g(x)$ como

$$R(f,g) = a^m b^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j)$$

Las siguientes propiedades de la resultante son bien conocidas y se puede consultar [La] ó [VdW] para las demostraciones.

(2.2) Proposición: Sean $f(x) = a \prod_{i=1}^{n} (x - \alpha_i)$; $g(x) = b \prod_{j=1}^{m} (x - \beta_j)$ polinomios separables sobre F . Entonces:

1) $R(g,f) = (-1)^{m \cdot n} R(f,g)$

2) Si $g(x) = f(x) \cdot q(x) + r(x)$ entonces
$R(f,g) = a^{m-\deg(r(x))} \cdot R(f,r)$

3) Si $f(x), g(x)$ tienen factores comunes, entonces
$R(f,g) = 0$

4) Si a,b son constantes no ambos 0 , entonces
$R(a,b) = 1$

5) Si $f(x) = f_1(x) \cdot f_2(x)$, entonces $R(f,f_2,g) =$
$= R(f_1,g) \cdot R(f_2,g)$

6) Si $g(x) = g_1(x) g_2(x)$, entonces $R(f,g_1 g_2) =$
$= R(f,g_1) R(f,g_2)$

7) $R(f,g) = a^m \prod_{i}^{n} g(\alpha_i) = (-1)^{m \cdot n} b^r \prod_{j}^{m} f(\beta_j)$

La siguiente propiedad de $R(f,g)$ será, más adelante, utilizada con frecuencia de modo que daremos una demostración de ella.

(2.3) Teorema: Sea $f(x)$ polinomio mónico separable de grado n con raíces $\alpha_1, \ldots, \alpha_n$. Entonces:

$$D(f) = R(f,f') = (-1)^{n\frac{(n-1)}{2}} R(f',f)$$

Demostración: Por (2.2)

$$R(f,f') = \prod_{k=1}^{n} f'(\alpha_k)$$

donde $$f(x) = \prod_{i=1}^{n} (x - \alpha_i)$$

se tiene $$f'(x) = \sum_j \prod_{i\neq j} (x - \alpha_i)$$

de modo que:

$$f'(\alpha_k) = \sum_j \prod_{i\neq j} (\alpha_k - \alpha_i) = \prod_{\substack{i \\ i\neq k}} (\alpha_k - \alpha_i)$$

y, por lo tanto

$$R(f,f') = \prod_i \prod_{\substack{i \\ i\neq k}} (\alpha_k - \alpha_i)$$

$$= \Big[\prod_{1\leq i<k\leq n} \prod (\alpha_k - \alpha_i)\Big]\Big[\prod_{1\leq k<i\leq n} (\alpha_k - \alpha_i)\Big]$$

$$= (-1)^{n\frac{(n-1)}{2}} D(f)$$

Usando el teorema anterior podemos encontrar la siguiente relación:

(2.4) Teorema: Sea $g(x)$ polinomio mónico, separable y $h(x)$ polinomio mónico separable. Entonces:

$$D(gh) = D(g)D(h)[R(h,g)]^2$$

Demostración: Se tiene por el teorema (2.3)

$$(-1)^{(i+j)(i+j-1)/2}D(gh) = R(gh,(gh)')$$

donde $i = \deg(g)$, $j = \deg(h)$. De esto resulta:

(2.4.1) $$R(gh,g'h + h'g) = R(g,g'h + gh')R(h,hg' + gh')$$

Pero α es raíz de $g(x)$, luego $g'(\alpha)h(\alpha) + h'(\alpha)g(\alpha) = g'(\alpha)h(\alpha)$. Luego (2.4.1) es equivalente a

$$R(g,g'h)R(h,gh')$$

$$= R(g,g')R(g,h)R(h,g)R(h,h')$$

$$= (-1)^{i(i-1)/2}D(g)R(g,h)(-1)^{ij}R(g,h)(-1)^{j(j-1)/2}D(h)$$

Pero $$\frac{(i + j)(i + j - 1)}{2} = \frac{i(i - 1)}{2} + ij + \frac{j(j - 1)}{2}$$

Por lo tanto: $(-1)^{i(i-1)/2}D(g)R(g,h)(-1)^{ij}R(g,h)(-1)^{j(j-1)/2}Dh$

$$= (-1)^{(i+j)(i+j-1)/2}D(g)D(h)[R(g,h)]^2$$

(ii) Estudiaremos ahora el caso car $F = 2$.

Sean $f(x),g(x) \in F[x]$ polinomios mónicos sin factor común

y separables. Entonces definamos una resultante aditiva $\tilde{R}(f,g)$ como un análogo a la resultante $R(f,g)$ en el caso car $F \neq 2$.

(2.5) Definición: Sean $f(x), g(x) \in F[x]$ polinomios mónicos separables y sin factor común. Sean $\alpha_1, \ldots, \alpha_n$ raíces de $f(x)$, $\beta_1, \ldots, \beta_j$ raíces de g . Entonces se define

$$\tilde{R}(f,g) = \sum_{i,j} \frac{\alpha_i}{\alpha_i + \beta_j}$$

(2.6) Observación: $\tilde{R}(f,g) \in F$ ya que permanece invariante bajo la acción del grupo de Galois $Gal(L/F)$ donde L es cuerpo de descomposición de $f(x)$ y $g(x)$.

Podemos demostrar ahora las siguientes propiedades:

(2.7) Proposición: Sean $f(x), g(x)$ como en (2.5). Entonces

1) $\tilde{R}(f,g) = n \cdot m + \tilde{R}(g,f)$; donde $n \cdot m \equiv 0$ ó $1 \pmod 2$

2) Si $f(x) = f_1(x) \cdot f_2(x)$ entonces $\tilde{R}(f,g) = \tilde{R}(f_1,g) + \tilde{R}(f_2,g)$

Demostración: (1) $\tilde{R}(f,g) = \sum_{i,j} \frac{\alpha_i}{\alpha_i + \beta_j}$

Pero:

$$\sum_{i,j} \frac{\alpha_i}{\alpha_i + \beta_j} = \frac{\alpha_1 \prod_{\substack{i \neq 1 \\ j \neq 1}} (\alpha_i - \beta_j) + \alpha_1 \prod_{\substack{i \neq 1 \\ j \neq 2}} (\alpha_i - \beta_j) + \ldots + \alpha_r \prod_{\substack{i \neq n \\ j \neq m}} (\alpha_i - \beta_j)}{\prod_{i,j} (\alpha_i - \beta_j)}$$

Como

$$R(f,g) = (\alpha_1 - \beta_1) \prod_{\substack{i\neq 1\\ j\neq 1}} (\alpha_i - \beta_j) = \alpha_1 \prod_{\substack{i\neq 1\\ j\neq 1}} (\alpha_i - \beta_j) + \beta_1 \prod_{\substack{i\neq 1\\ j\neq 1}} (\alpha_i - \beta_j)$$

y reemplazando en cada caso

$$\widetilde{R}(f,g) = \frac{R(f,g) + \beta_1 \prod_{\substack{i\neq 1\\ j\neq 1}} (\alpha_i - \beta_j)}{R(f,g)} + \frac{R(f,g) + \beta_2 \prod_{\substack{i\neq 1\\ j\neq 2}} (\alpha_i - \beta_j)}{R(f,g)} +$$

$$+ \ldots + \frac{R(f,g) + \beta_m \prod_{\substack{i\neq n\\ j\neq m}} (\alpha_i - \beta_j)}{R(f,g)}$$

$$= n\cdot m + \widetilde{R}(g,f)$$

como car F = 2 tomamos $\overline{n\cdot m}(\text{mod } 2)$.

(2) $$\widetilde{R}(f,g) = \sum_{i,j} \frac{\alpha_i}{\alpha_i + \beta_j}$$

si $\alpha_1, \ldots, \alpha_k$ son raíces de $f_1(x)$ y $\alpha_{k+1}, \ldots, \alpha_n$ son raíces de $f_2(x)$.

Entonces

$$\widetilde{R}(f,g) = \sum_{j=1}^{n} \sum_{i=1}^{k} \frac{\alpha_i}{\alpha_i + \alpha_j} + \sum_{j=1}^{k} \sum_{i=k+1}^{n} \frac{\alpha_i}{\alpha_i + \alpha_j}$$

$$= \widetilde{R}(f_1,g) + \widetilde{R}(f_2,g) .$$

(2.8) Proposición: Bajo las mismas hipótesis, se tiene:

$$\widetilde{R}(f,g) = \frac{\sum_i \alpha_i g'(\alpha_i) \prod_{i\neq k} g(\alpha_k)}{R(f,g)}$$

Demostración: $\widetilde{R}(f,g) = \sum_{i,j} \frac{\alpha_i}{\alpha_i + \beta_j} =$

$$= \frac{\alpha_1 \prod_{\substack{i\neq 1\\ j\neq 1}} (\alpha_i-\beta_j) + \alpha_1 \prod_{\substack{i\neq 1\\ j\neq 2}} (\alpha_i-\beta_j) + \ldots + \alpha_n \prod_{\substack{i\neq n\\ j\neq m}} (\alpha_i-\beta_j)}{\prod_{i,j} (\alpha_i - \beta_j)} =$$

$$= \frac{\alpha_1\left[\sum_{j=1}^{m} \prod_{i\neq j} (\alpha_1-\beta_i) \prod_{k\neq 1} g(\alpha_k)\right]}{R(f,g)} + \frac{\alpha_2\left[\sum_{j=1}^{m} \prod_{i\neq j} (\alpha_2-\beta_i) \prod_{k\neq 2} g(\alpha_k)\right]}{R(f,g)} +$$

$$+ \ldots\ldots + \frac{\alpha_n\left[\sum_{j=1}^{m} \prod_{i\neq j} (\alpha_n - \beta_i) \prod_{k\neq n} g(\alpha_k)\right]}{R(f,g)} =$$

$$= \frac{\sum_i \alpha_i g'(\alpha_i) \prod_{k\neq i} g(\alpha_k)}{R(f,g)}$$

Obtenemos entonces el siguiente corolario:

(2.9) Corolario: Sea $f(x) \in F[x]$ mónico y separable. Entonces:

$$\widetilde{R}(f,f') = 0$$

Demostración: $\tilde{R}(f,f') = \dfrac{\sum_i \alpha_i f''(\alpha_i) \prod_{i\neq k} f(\alpha_k)}{R(f,g)}$

Pero como car F = 2 tenemos $f''(x) = 0$, luego

$$\tilde{R}(f,f') = 0$$

Demostraremos ahora una propiedad de $\tilde{R}$ análoga a (2.4) que justifica el nombre de resultante aditiva de dos polinomios $f(x),g(x) \in F[x]$.

(2.10) Teorema: Sean $f(x),g(x) \in F[x]$ mónicos, separables y sin factor común. Entonces

$$D(f\cdot g) = D(f) + D(g) + [\tilde{R}(f,g)]^2 + \tilde{R}(f,g)$$

Demostración: Sean $\alpha_1, \ldots, \alpha_n$ las raíces de $f(x)$

$\beta_1, \ldots, \beta_s$ las raíces de $g(x)$

Entonces $f(x)\cdot g(x) = (x - \alpha_1) \ldots (x - \alpha_n)(x - \beta_1) \ldots (x - \beta_s)$ se tiene:

$$D(f\cdot g) = \sum_{1\leq i<j\leq n} \frac{\alpha_i\alpha_j}{(\alpha_i+\alpha_j)^2} + \sum_{1\leq i<j\leq s} \frac{\beta_i\beta_j}{(\beta_i+\beta_j)^2} + \sum_{\ell,s} \frac{\alpha_\ell\beta_s}{\alpha_\ell+\beta_s}$$

$$= D(f) + D(g) + \sum_{\ell,s} \frac{\alpha_\ell\beta_s}{\alpha_\ell + \beta_s}$$

Donde α_ℓ recorre todas las raíces de f y β_s todas las

Por otra parte:

$$[\tilde{R}(f,g)]^2 + \tilde{R}(f,g) = \sum_{\ell,s} \left(\frac{\alpha_\ell^2}{(\alpha_\ell + \beta_j)^2} + \frac{\alpha_\ell}{\alpha_\ell + \beta_j} \right)$$

$$= \sum_{\ell,s} \frac{\alpha_\ell \beta_s}{\alpha_\ell^2 + \beta_j^2}$$

Por lo tanto:

$$D(f \cdot g) = D(f) + D(g) + [\tilde{R}(f,g)]^2 + \tilde{R}(f,g)$$

Aplicando ahora las propiedades anteriores, tenemos el si - guiente ejemplo:

Sea $f(x) = x^n - a^n \in F[x]$; $g(x) = x^n - b^n \in F[x]$ car $F = 2$ n,m impares. Entonces:

$$\tilde{R}(f,g) = \frac{\sum_i a_i g'(a_i) \prod_{i \neq k} g(a_k)}{R(f,g)}$$

$$= \frac{\sum_{i=0} a_i \prod_{i \neq k} ((a_k)^m - b^n) m a_i^{m-1}}{R(f,g)}$$

donde a_i son las raíces de $f(x)$.

Sea ξ raíz n-ésima de la unidad. Entonces se tiene:

$$x^n - a^n = \prod_{i=1}^{n} (x - a\xi^i)$$

Luego:

$$\widetilde{R}(f,g)R(f,g) = \sum_{i=0}^{n-1} (\xi^i a) \prod_{\substack{k=0 \\ k\neq i}}^{n-1} ((\xi^k a)^m - b^n) m (\xi^i a)^{m-1}$$

$$= m \sum_{i=0}^{n-1} (\xi^i a)^m \prod_{\substack{k=0 \\ k\neq i}}^{n-1} ((\xi^k a)^n - b^m)$$

$$= \sum_{i=0}^{n-1} ((\xi^i a)^m + b^m + b^n) \prod_{\substack{k=0 \\ k\neq i}}^{n-1} ((\xi^k a)^m - b^m)$$

$$= m \sum_{i=0}^{n-1} g(a_i) \prod_{\substack{k=0 \\ k\neq i}}^{n-1} g(a_k) + b^m \sum_{i=0}^{n-1} \prod_{k\neq i} ((\xi^k a)^m - b^m)$$

$$= n\cdot m\, R(f,g) + m b^m a^{m(n-1)} h' \left| \left(\frac{b}{a}\right)^m \right|$$

donde $h(Y) = \prod_{k=0}^{n-1} (c^k - Y)$; $c = \xi^n$.

Luego

$$R(f,g)R(f,g) = R(f,g)n\cdot m + m b^m a^{m(n-1)} h' ((\tfrac{b}{a})^m)$$

Pero como $n\cdot m \equiv 1 \pmod 2$ y $m \equiv 1 \pmod 2$

$$\widetilde{R}(f,g) = \frac{1 + b^m a^{m(n-1)} h' ((\frac{b}{a})^m)}{R(f,g)}$$

Más adelante en § 4 demostraremos que para f,g como en el ejemplo, $R(f,g) = (-1)(a^k - b^k)^d$ donde $d = \text{mcd}(n,m)$; $k = n \cdot m/d$. Luego utilizando este resultado tenemos:

$$\tilde{R}(f,g) = \frac{1 + b^m a^{m(n-1)} h'((\frac{b}{a})^m)}{(a^k - b^k)^d}$$

§ 3. Relación de la discriminante usual con la discriminante de Berlekamp.

En este párrafo se introducirá una relación, a través de un homomorfismo, entre la discriminante de un polinomio sobre un cuerpo cualquiera y la discriminante de Berlekamp para el caso de característica 2. Este homomorfismo ha sido introducido por Wadsworth en [Wads] y tiene la ventaja de permitir estudiar la discriminante de Berlekamp en característica 2 a partir de la discriminante usual en característica 0.

Sea F cuerpo de característica 2. Entonces existe anillo de valuación discreta (Henseliano) V con cuerpo residual F, car $V = 0$ y uniformizante $= 2$ (Ver [Se] y [Gr])

Sea $V^* = V/2V$ el grupo de unidades de V

$K = \mathrm{Quot}(V)$

$v : K^* \to \mathbb{Z}$ la valuación asociada a V

Observación: Como 2 es uniformizante se tiene: $v(2) = 1$

Luego $-1 \notin K^{*2}$ pués:

Si $-1 = i^2$ entonces $v(i^2) = 2(v(i)) = v(-1) = 0$

Luego $v(i) = 0$. Como $(i + 1)^2 = 2i$ se tiene:

$$v((i + 1)^2) = 2(v(i + 1))$$

$$= v(2i)$$

$$= 2(v(i + 1)) = v(2) + v(i) = 1$$

Luego $v(i + 1) = 1/2$

Luego $-1 \notin K^{*2}$.

(3.1) Definición: Sea $S := \{(-1)^k a^2 + 4b/k \in \mathbb{Z}\ ,\ a \in V^*,\ b \in V\}$ el subgrupo multiplicativo de V^* de los elementos discriminantes de V .

Introduciremos ahora un epimorfismo que denotaremos γ y que será el que relacione la discriminante usual con la discriminante de Berlekamp.

(3.2) Lema: Sea $\gamma : S \to F/p(F)$ definido por:

$$\gamma((-1)^k a^2 + 4b) = \frac{\bar{b}}{\bar{a}^2} \pmod{p(F)}$$

donde $\bar{b}, \bar{a}$ son las clases módulo 2 de a,b en F .

Entonces γ es epimorfismo de grupos y $\ker \gamma = \pm V^{*2}(1 + 8V)$

Si V es Henseliano, se tiene $\ker \gamma = \pm V^{*2}$

Demostración: Demostraremos primero que γ está bien definida.

Supongamos $(-1)^k a^2 + 4b = (-1)^{k'} a'^2 + 4b'$; $k,k' \in \mathbb{Z}$; $a,a' \in V^*$; $b,b' \in V$

Entonces reduciendo módulo 2

$$\bar{a} = \bar{a}'$$

Luego

$$a' = a + 2c \quad , \quad a \in V$$

Entonces:

$$4(b - b') = [-(-1)^k + (-1)^{k'}]a^2 + (-1)^{k'}(4ac + 4c^2)$$

Pero $2a^2 \notin 4V$, luego:

$$(-1)^{k'} = (-a)^k \quad y \quad b' = b \pm (ac + c^2)$$

Luego en $F/p(F)$: $$\frac{\bar{b}'}{\bar{a}'^2} = \frac{\overline{[b \pm (c^2 + ac)]}}{\bar{a}^2}$$

$$= \frac{\bar{b}}{\bar{a}^2} + \left[\left(\frac{\bar{c}}{\bar{a}}\right)^2 + \left(\frac{\bar{c}}{\bar{a}}\right)\right] = \frac{\bar{b}}{\bar{a}^2}$$

Luego γ está bien definida

Sean $(-1)^k a^2 + 4b$; $(-1)^{k'} a'^2 + 4b' \in S$; $k,k' \in \mathbb{Z}$;

$a,a' \in V^*$; $b,b' \in V$. Entonces

$$\gamma((-1)^k a^2 + 4b)((-1)^{k'} a'^2 + 4b')$$

$$= \gamma((-1)^{k+k'} a^2 a'^2 + (-1)^k a^2 4b' + (-1)^{k'} a'^2 4b + 16bb')$$

$$= \gamma((-1)^{k''} a''^2 + 4((-1)^k a^2 b' + (-1)^{k'} a'^2 b + 4bb')$$

donde $a'' = (aa')$; $k'' = k + k'$

$$= \frac{\overline{(-1)^k a^2 b' + (-1)^{k'} a'^2 b + 4bb'}}{\bar{a}''^2}$$

$$= \frac{\overline{a'^2 b' + ba'^2}}{\overline{a''^2}}$$

Por otra parte:

$$\gamma((-1)^k a^2 + 4b) + \gamma((-1)^{k'} a'^2 + 4b')$$

$$= \frac{\overline{b}}{\overline{a}^2} + \frac{\overline{b'}}{\overline{a''}^2} \equiv \frac{\overline{ba'^2 + a^2 b'}}{\overline{a''2}}$$

Luego γ es homomorfismo de grupos.

Demostraremos que γ es epimorfismo.

Sea $a \in F/p(F)$ y tomemos $b \in F$ con

$$b(\text{mod } p(F)) = a$$

como $b \in F$, sea $c \in V$ pre-imagen de b y consideremos el elemento

$$(-1)^k + 4c \in S$$

Entonces $\gamma((-1)^k + 4c) = \overline{c}(\text{mod } p(F)) = a$

luego γ es epimorfismo.

Calculemos ahora $\ker \gamma$

Por una parte se tiene claramente $\pm V^{*2}(1 + 8V) \subseteq \ker \gamma$

ahora sin pérdida de generalidad consideremos elementos $(\pm 1 + 4b) \in S \cap \ker \gamma$.

Entonces $\gamma(\pm 1 + 4b) = \overline{b} = \overline{0}(\text{mod } p(F))$

es decir existe $c \in V$ con $\overline{b} = \overline{c}^2 + \overline{c}$ en F

Luego $b = c^2 + c + 2d$ en V

por lo tanto $\pm 1 + 4b = \pm 1 + 4(c^2 + c + 2d)$

$= \pm 1 + 8d + 4c(c + 1)$

Pero $(2c + 1)^2 = 4c^2 + 4c + 1$

Luego en el caso: $+1 + 4b = 8d + (1 + 2c)^2 \in V^{*2}(1 + 8V)$

y en el caso: $-1 + 4b = 8d + 8c^2 - (-1 - 2c)^2 \in V^{*2}(1 + 8V)$

Luego $\ker \gamma = V^{*2}(1 + 8V)$. Si V es henseliano, entonces $(1 + 8V) \subseteq V^{*2}$ y por lo tanto:

$$\ker \gamma = \pm V^{*2}$$

tenemos entonces que γ induce un isomorfismo $\overline{\gamma} : S/V^{*2} \to F/p(F)$ que también denotaremos por γ.

Consideremos ahora $\overline{f}(t) \in F[t]$ polinomio separable $\overline{f}(t) = \overline{a}_n t^n + \ldots + \overline{a}_o$, $\overline{a}_i \in F = V/2V$; $\overline{a}_n \neq 0$.

Sea $a_i \in V$ representante de $\overline{a}_i$ para $0 \leq i \leq n$ y sea $f(t) = a_n t^n + \ldots + a_o \in V[t]$ con $a_n \in V^*$ pues $\overline{a}_n \neq 0$. Entonces $f(t) \in V[t]$ es un levantamiento de $\overline{f}(t)$ cuya reducción módulo 2 es $\overline{f}(t)$.

Demostraremos que el levantamiento $f(t)$ de $\overline{f}(t)$ es tam - bién separable, y que las raíces de $f(t)$ se reducen módulo 2 a las raíces de $\overline{f}(t)$.

Sea $K = \mathrm{Quot}(V)$ y sea N el cuerpo de descomposición de

de $f(t)$ sobre K, es decir, se tiene $N = K(\alpha_1, \ldots, \alpha_n)$ donde $f(t) = a_n \prod_{i=1}^{n} (t - \alpha_i)$, $\alpha_1, \ldots, \alpha_n \in N$.

Demostraremos que $\alpha_i \neq \alpha_j$ para todo i,j lo que implica que f es separable.

Pero para todo i se tiene:

$$a_n \alpha_i^n + \ldots + a_o = 0$$

es decir:

$$\alpha_i^n + \frac{a_{n-1}}{a_n} \alpha_i^{n-1} + \ldots + \frac{a_o}{a_n} = 0$$

y con $\frac{a_{n-1}}{a_n}, \ldots, \frac{a_o}{a_n} \in V$ pués $a_n \in V^*$.

Luego α_i es entero sobre V para todo $1 \leq i \leq n$. Sea B la cerradura entera de V en N. Se tiene entonces $\alpha_1, \ldots, \alpha_n \in B$, por lo tanto $V[\alpha_1, \ldots, \alpha_n] \subseteq B$.

Pero la valuación v de K se prolonga a N (en forma única si V es henseliano), definiendo para todo $\alpha \in N$.

$$v(\alpha) = v\left[N_{N/K}(\alpha)\right]^{1/n}$$

donde $N_{N/K} : N \to K$ es la norma de N/K. B está contenido en el anillo de valuación de v (para todo v). Sea $\overline{N}$ el cuerpo residual de (N,v). Sean $\overline{\alpha_1}, \ldots, \overline{a_n} \in \overline{N}$ las imagenes de $\alpha_1, \ldots, \alpha_n$. Como $f(t) = a_n \prod_{i=1}^{n} (t - \alpha_i) \in B[t]$

Entonces la reducción de $f(t)$ en $\overline{N}$ es:

$$\overline{f}(t) = \overline{a}_n \prod_{i=1}^{n} (t - \overline{\alpha}_i)$$

Pero $\overline{f}(t)$ es separable, es decir, se tiene $\overline{\alpha_i} \neq \overline{\alpha_j}$ para todo $i \neq j$. Luego $\alpha_i \neq \alpha_j$ para todo $i \neq j$. Más aún, se vé que $\alpha_i \pm \alpha_j$ es una unidad en B todo $i \neq j$. Por lo tanto $f(t) \in V[t]$ es separable y en consecuencia N/K es galoisiana.

Ahora el discriminante de $f(t)$ en el sentido usual es:

$$\Delta(f(t)) = \prod_{i<j} (\alpha_i - \alpha_j)^2 \in V^* / V^{*2}$$

pués $\prod_{i<j} (\alpha_i - \alpha_j)^2 \in V^*$. Luego si alteramos $\Delta(f(t))$ por un cuadrado de V^* no cambia la clase $\overline{\Delta}(f(t))$ mod V^* / V^{*2} .

Pero $\prod_{i<j} (\alpha_i + \alpha_j) \in V^*$ pués:

i) $\prod_{i<j} (\alpha_i + \alpha_j) \in V$ ya que está en K y es entero

ii) $\prod_{i<j} (\alpha_i + \alpha_j) \to \prod_{i<j} (\overline{\alpha_i} + \overline{\alpha_j}) \neq 0$ luego pertenece a V^*

Es decir: $\prod_{i<j} (\alpha_i + \alpha_j)^2 \in V^{*2}$

Alteremos, entonces, la clase mod V^{*2} de $\Delta(f(t))$ por $\prod_{i<j} (\alpha_i + \alpha_j)^{-2}$

$$\Delta(f(t)) = \prod_{i<j} (\alpha_i - \alpha_j)^2 \prod_{i<j} (\alpha_i + \alpha_j)^{-2} \in V^* \quad V^{*2}$$

$$= \prod_{i<j} \left(\frac{\alpha_i - \alpha_j}{\alpha_i + \alpha_j} \right)^2$$

$$= \prod_{i<j} \left(1 - \frac{4\alpha_i\alpha_j}{(\alpha_i + \alpha_j)^2} \right)$$

$$= [\, 1 - 4 \left(\sum_{i<j} \frac{\alpha_i\alpha_j}{(\alpha_i + \alpha_j)^2} + 4\beta \right] \in V^* \quad V^{*2} ,$$

$\beta \in V$.

Luego $\Delta(f(t)) \in S_{V^{*2}}$ y además:

$$\gamma(\Delta(f(t)) = \Sigma \frac{\overline{\alpha_i\alpha_j}}{(\overline{\alpha_i} + \overline{\alpha_j})^2} = D(f(t))$$

Luego tenemos el siguiente lema:

(3.3) Lema: Si $\overline{f}(t) \in F[t]$ es separable y $f(t) \in V(t)$ es un levantamiento de $\overline{f}(t)$ cualquiera del mismo grado, entonces

$$\gamma(\Delta(f(t)) = D(\overline{f}(t))$$

§ 4. Aplicaciones de la relación entre la discriminante usual y la discriminante de Berlekamp.

En este párrafo estudiaremos algunas aplicaciones del método introducido en §3 .

La primera será calcular la discriminante de Berlekamp para un trinomio $f(x) = x^n + ax^k + b \in F[x]$, n,k no simultáneamente pares, car $F = 2$. Para esto utilizaremos el cálculo de la discriminante usual para un trinomio de este tipo sobre un cuerpo cualquiera hecho por Swan [Be]$_1$. Usando este resultado estudiaremos la paridad de la cantidad de factores irreducibles que se obtienen al descomponer el trinomio $f(x)$ sobre $GF(2^m)$ usando el criterio de Stickelberger-Berlekamp (Ver [Be]$_1$).

Demostraremos primero el siguiente lema:

(4.1) Lema (Swan): Sea $f(x) = x^j - \xi^j$; $g(x) = x^k - \nu^k \in F[x]$ entonces $R(x^j - \xi^j, x^k - \nu^k) = (-1)^j(\nu^m - \xi^m)^d$ donde $d = mcd(j,k)$, $m = \frac{jk}{d}$.

Demostración: Sea α j-ésima raíz primitiva de la unidad, entonces

$$x^j - \xi^j = \prod_{i=1}^{j} (x - (\xi\alpha)^i)$$

$$R(x^j - \xi^j, x^k - \nu^k) = \prod_{i=1}^{j} ((\xi\alpha^i)^k - \nu^k)$$

$$= (-1)^k \xi^{md} \prod_{i=1}^{j} ((\tfrac{\nu}{\xi})^k - \alpha^{ki})$$

Como α^k tiene orden j/α

$$\prod_{i=1}^{j/d} (x - \alpha^{ki}) = x^{j/d} - 1 \qquad \text{y además}$$

$$R(x^j - \xi^j, x^k - \nu^k) = (-1)^j \xi^{md} [\,(\tfrac{\nu}{\xi})^{jk/d} - 1]^d$$

$$= (-1)^j (\nu^m - \xi^m)^d$$

Podemos demostrar ahora el teorema de Swan.

(4.2) Teorema (Swan): Sea $n > k > 0$, sea $d = mcd(r,k)$ $n = Nd$, $k = Kd$, entonces la discriminante del trinomio $x^n + ax^k + b \in F[x]$, F cuerpo cualquiera, está dada por:

$$\Delta(x^n + ax^k + b) = (-1)^{n(n-1)/2} b^{k-1} (n^N b^{N-K} - (-1)^N (n-k)^{N-K} k^K a^N)^d$$

Demostración: Si $f(x) = x^n + ax^k + b$, entonces

$$\Delta(f(x)) = (-1)^{n(n-1)/2} R(nx^{n-1} + akx^{k-1}, f(x)) \quad \text{(por §2(2.3))}$$

Pero

$$R(nx^{n-1} + akx^{k-1}, f(x)) = R(x^{b-1}, f(x) R(n, f(x)) R(x^{n-k} + n^{-1}ak, f(x))$$

Calculando cada resultante:

$$R(x^{k-1}, f(x)) = (f(0))^{k-1} = b^{k-1}$$

$$R(n, f(x)) = n^n = n^{Nd}$$

$$R(x^{n-k} + n^{-1}ak, f(x)) = R(x^{n-k}+n^{-1}ak, x^k(x^{n-k}+n^{-1}ak) +$$

$$+ a(1-n^{-1}k)x^k+b)$$

$$= R(x^{n-k} + n^{-1}ak, a(1 - n^{-1}k)x^k + b)$$

$$= (a(1-n^{-1}k))^{n-k}R(x^{n-k}-\xi^{n-k}, x^k-\nu^k)$$

donde $\xi = (-n^{-1}ak)^{1/(n-k)}$

$$\nu = (ba^{-1}(n^{-1}k - 1)^{-1})^{1/k}$$

Utilizando el lema y poniendo

$$J = n - k$$

$$m = (N - K)Kd$$

$$\nu^m = (ba^{-1}(n^{-1}k - 1)^{N-K}$$

$$\xi^m = (-n^{-1}ak)^K$$

obtenemos el resultado del teorema.

Consideremos ahora $f(x) = x^n + ax^k + b \in F[x]$, car F = 2 separable, es decir, n,k no simultáneamente pares. Calcularemos la discriminante de Berlekamp D(f(x)) utilizando el párrafo § 3.

Sea, como en § 3, V anillo de valuación discreta con car V = 0 , 2V el ideal maximal y F = V/2V . Denotaremos también por $f(x) = x^n + ax^k + b \in V[x]$ un levantamiento de f(x) de V . Consideremos separadamente los casos

n impar y k par; n par y k impar y ambos impares:

I. $n = 2s + 1$ $\quad n = Nd \quad N = 2\ell + 1$

$k = 2t \quad k = Kd \quad K = 2r$

$d = (n,k) \quad d = 2p + 1$

Por teorema (4.2) en V se tiene:

$$\Delta(f(x)) = \pm b^{2t-1}(n^{2\ell+1}b^{2(\ell-r)+1} + (n - k)^{2(\ell-r)+1}(2t)^{2n}a^{2\ell+1})d$$

Pero $\Delta(f(x))$ se define módulo cuadrados, luego: sin perder generalidad, como d es impar, consideremos el exponente = 1

$$\Delta(f(x)) = \pm b^{2t-1}(n^{2\ell+1}b^{2(\ell-r)+1}b^{2(\ell-r)+1} + (n-k)^{2(\ell-r)+1}(2t)^{2r}a^{2\ell+1})$$

$$= \pm(b^{2t}n^{2\ell+1}b^{2(\ell-r)+2}) + k^{2t}b(n-k)^{2(\ell-r)+1}(2t)^{2r}a^{2\ell+1})$$

Si $n \equiv \pm 1 \pmod 4$, $n = \pm 1 + 4u$ entonces se obtiene:

$$\Delta(f(x)) = \pm(b^{t+(\ell-r)+1}n^{\ell})^2 \pm 4(u(b^{t+(\ell-r)+1}n^{\ell})^2 +$$

$$+ b^{2t+1}(n - k)^{2(\ell-r)+1}.4^{r-1}t^{2\ell}a^{2\ell+1}) \in S \quad \text{(ver § 3)}.$$

Aplicando el homomorfismo γ, introducido en § 3 se tiene:

i) $r > 1$ es decir $K > 2$

$\gamma(\Delta(f(x)) = \bar{u} \pmod 2$

ii) $r = 1$ es decir $K = 2$.

$$\gamma(\Delta(f)) = \gamma(\pm b^{t+\ell} n^{\ell})^2 \pm 4(u(b^{t+\ell} n^{\ell})^2 + b^{2t+1}(n-k)^{2\ell-1} t^2$$

$$= \bar{u} + \frac{b^{2t+1}(\overline{n-k})^{2\ell-1} t^2 a^{2\ell+1}}{b^{2t+2\ell} n^{2\ell}}$$

$$= \bar{u} + \frac{b(\overline{n-k})^{2\ell-1} t^2 a^{2\ell+1}}{b^{2\ell} n^{2\ell}}$$

$$= \bar{u} + \frac{a^{2\ell+1}}{b^{2\ell-1}}$$

$$= \bar{u} + \frac{a^{n/d}}{b^{n/d-2}} \qquad \text{en} \quad F/p(F)$$

II. $n = 2s$ $\qquad N = 2\ell$

$k = 2t + 1$ $\qquad K = 2r - 1$

$d = (n,k)$ $\qquad d = 2p + 1$

$$\Delta(f(x)) = (-1)^{\frac{n(n-1)}{2}} [b^{2t}(2s)^{2\ell} b^{2(\ell-r)+1} - (n-k)^{2(\ell-r)+1} k^{2r-1} a^{2\ell}]$$

$$= \pm(b^{2t} 4^{\ell} s^{2\ell} b^{2(\ell-r)+1}) \pm b^{2t}(n-k)^{2(\ell-r)+1} k^{2r-1} a^{2\ell}$$

$$= \pm(b^{2t} 4^{\ell} s^{2\ell} b^{2(\ell-r)+1} + b^{2\ell}(n-k)^{2(\ell-r)} k^{2r} a^{2\ell}(n-k)k^{-1}$$

Como la discriminante $\Delta(f(x))$ se define módulo cuadrados, alterando la expresión anterior por k^2 se tiene:

$$\Delta(f(x)) = \pm b^{2t} 4^{\ell} s^{2\ell} b^{2(\ell-r)+1} k^2 - b^{2t}(n-k)^{2(\ell-r)} k^{2r} a^{2\ell}(n-k)k$$

Ahora si $(n - k)k \equiv \pm 1 \pmod 4$, es decir, $(n - k)k = \pm 1 + 4v$, $v \in \mathbb{Z}$, se tiene:

$$\Delta(f(x)) = \pm(b^t(n-k)^{\ell-r} k^r a^{\ell})^2(1+4v) + 4(4^{\ell-1} b^{2t} s^{2\ell} b^{2(\ell-r)+1})$$

$$= \pm(b^t(n-k)^{\ell-r} k^r a^{\ell})^2 + 4(v(b^t(n-k)^{\ell-r} k^r a^{\ell})^2 + 4^{\ell-1} b^{2t} \cdot s^{2\ell} b^{2(\ell-r)+1}).$$

i) $\ell > 1$ entonces $N > 2$ y aplicando γ

$$\gamma(\Delta(f(x)) = \bar{v} \pmod 2$$

ii) $\ell = 1$ tenemos $N = 2$ y aplicando el homomorfismo γ

$$\gamma(\Delta(f(x)) = \gamma(b^t(n-k)^{1-r} k^r a^{\ell})^2 + 4(v(b^t(n-k)^{1-r} k^r a^{\ell})^2 + b^{2t} s^2 b^{2(1-r)+1} . k^2)$$

$$= \bar{v} + \frac{\bar{s}^2 b^{3-2r}}{(\overline{n - k})^{2(1-r)} \bar{k}^{2r} a^{2\ell}}$$

$$= \bar{v} + \frac{b^{2-k/d}}{a^2}$$

III. $n = 2s + 1$ $\qquad N = 2\ell + 1$

$k = 2t + 1$ $\qquad K = 2r + 1$

$d = (n,k)$ $\qquad d = 2p + 1$

$$\Delta(f(x)) = \pm b^{2t}(n^{2\ell+1}b^{2(\ell-r)} + (n-k)^{2(\ell-r)}k^{2r+1}a^{2\ell+1}$$

$$= \pm b^{2t}(n^{2\ell+1}b^{2(\ell-r)} \mp ((2(s-t))^{2(\ell-r)}k^{2r+1}a^{2\ell+1})$$

$$= \pm b^{2t}n^{2\ell}b^{2(\ell-r)}n \pm 4^{\ell-r}(s-t)^{2(\ell-r)}k^{2r+1}a^{2\ell+1}b^{2t}$$

y $n = \pm 1 + 4w$, $w \in \mathbb{Z}$

Entonces:

$$\Delta(f(x) = \pm b^{2t}n^{2\ell}b^{2(\ell-r)} \pm 4(wb^{2t}n^{2\ell}b^{2(\ell-r)} + 4^{\ell-r-1}(s-t)^{2(\ell-r)})$$

i) $\ell - r - 1 > 0$, es decir $\ell - r > 1$.

Entonces $\gamma(\Delta(f(x)) = \overline{w}(\text{mod } 2)$

ii) $\ell - r - 1 = 0$, es decir $\ell - r = 1$.

Entonces:

$$\gamma(\Delta(f(x)) = \overline{w} + \frac{(\overline{s-t})\, a^{2\ell+1}}{b^{2(\ell-r)}}$$

$$= \begin{cases} \overline{w} & \text{si } (s-t) \equiv 0(\text{mod } 2) \\ \overline{w} + \dfrac{a^{2\ell+1}}{b^2} & \text{si } (s-t) \equiv 1(\text{mod } 2) \end{cases}$$

Hemos demostrado entonces:

(4.3) Teorema: Sea $f(x) = x^n + ax^k + b$ polinomio separable sobre F , car $F = 2$. Entonces si $d = (n,k)$, $n = Nd$, $k = Kd$ la discriminante de Berlekamp de $f(x)$ es:

Si n impar, k par

$$D(f(x)) = \begin{cases} 0 & \text{si } n \equiv \pm 1 \pmod 8, \quad K > 2 \\ 1 & \text{si } n \equiv \pm 3 \pmod 8, \quad K > 2 \\ \dfrac{a^{n/d}}{b^{(n/d)-2}} & \text{si } n \equiv \pm 1 \pmod 8, \quad K = 2 \\ 1 + \dfrac{(a^{n/d})}{b^{(n/d)-2}} & \text{si } n \equiv \pm 3 \pmod 8, \quad K = 2 \end{cases}$$

n par, k impar

$$D(f(x)) = \begin{cases} 0 & \text{si } (n-k)k \equiv \pm 1 \pmod 8, \quad N > 2 \\ 1 & \text{si } (n-k)k \equiv \pm 3 \pmod 8, \quad N > 2 \\ \dfrac{b^{2-k/d}}{a^2} & \text{si } (n-k)k \equiv \pm 1 \pmod 8, \quad N = 2 \\ 1 + \dfrac{b^{2-k/d}}{a^2} & \text{si } (n-k)k \equiv \pm 3 \pmod 8, \quad N = 2 \end{cases}$$

Si n impar, k impar

$$D(f(x)) = \begin{cases} 0 & \text{si } n \equiv \pm 1 \pmod 8 \ , \ N - K > 2 \\ 1 & \text{si } n \equiv \pm 3 \pmod 8 \ , \ N - K > 2 \\ 0 & \text{si } (n-k) \equiv 0 \pmod 4 \ , \ n \equiv \pm 1 \pmod 8 \ , \ N-K = 2 \\ 1 & \text{si } (n-k) \equiv 0 \pmod 4 \ , \ n \equiv \pm 3 \pmod 8 \ , \ N-K = 2 \\ \frac{a^N}{b^2} & \text{si } (n-k) \equiv 1 \pmod 4 \ , \ n \equiv \pm 1 \pmod 8 \ , \ N-K = 2 \\ 1 + \frac{a^N}{b^2} & \text{si } (n-k) \equiv 1 \pmod 4 \ , \ n \equiv \pm 3 \pmod 8 \ , \ N-K = 2 \end{cases}$$

Como segunda aplicación del párrafo § 3 determinaremos la paridad de la cantidad de factores irreducibles que se obtienen al descomponer el trinomio $x^n + ax^k + b$ sobre $GF(2^m)$ con lo cual se generaliza el corolario (6.696) de [Be]$_1$ que solo trata el trinomio $x^n + x^k + 1$ sobre $GF(2)$.

Para esta aplicación utilizaremos el teorema siguiente que es la versión en característica 2 del teorema de Stickelberger (Ver [Be]$_1$).

(4.4.) Teorema: Si $f(x)$ es un polinomio de grado m que es el producto de r polinomios irreducibles y distintos sobre $GF(2^n)$, entonces

$$r \equiv m \pmod 2 \quad \text{si y sólo si } Tr(D(f(x))) = 0$$

Donde $$Tr(x) = \sum_{i=0}^{n-1} x^{2^i}$$

La demostración del teorema (4.4) se basa en los siguientes lemas:

(4.5) Lema: $$Tr(D(f(x))) = \sum_{1\leq i<j\leq m} \left[\frac{1}{1 + \alpha_j/\alpha_i} + \frac{1}{1 + (\alpha_j/\alpha_i)^q}\right]$$

donde $q = 2^n$.

Demostración: En un cuerpo de característica dos se tienen:

$$\frac{\alpha_i\alpha_j}{(\alpha_i + \alpha_j)^2} = \frac{\alpha_j/\alpha_i}{1 + (\alpha_j/\alpha_i)^2} = \frac{1}{1 + \alpha_j/\alpha_i} + \frac{1}{1 + (\alpha_j/\alpha_i)^2}$$

y por lo tanto

$$Tr(D(f)) = \sum_{k=0}^{n-1} \sum_{1\leq i<j\leq m} \left[\frac{1}{1 + \alpha_j/\alpha_i} + \frac{1}{1 + (\alpha_j/\alpha_i)^2}\right]^{2k}$$

$$= \sum_{1\leq i<j\leq m} \sum_{k=0}^{n-1} \left[\frac{1}{1 + (\alpha_j/\alpha_i)^{2^k}} + \frac{1}{1 + (\alpha_j/\alpha_i)^{2^{k+1}}}\right]$$

$$= \sum_{1\leq i<j\leq m} \left(\frac{1}{1 + \alpha_j/\alpha_i} + \frac{1}{1 + (\alpha_j/\alpha_i)^q}\right)$$

(4.6) Lema: El teorema (4.4) es cierto si $r = 1$.

Demostración: Si $r = 1$, $f(x)$ es irreducible y $\alpha_i = \alpha^{q^i}$

Luego:

$$\mathrm{Tr}(D(f)) = \sum_{1 \le i < j \le n} \left(\frac{1}{1 + \alpha^{q^i}} + \frac{1}{1 + \alpha^{q(q^j - q^i)}} \right)$$

Poniendo $J = j - i$ se tiene:

$$\mathrm{Tr}(D(f)) = \sum_{j=1}^{m-1} \sum_{i=1}^{m-j} \left(\frac{1}{1 + \alpha^{q^j(q^j-1)}} + \frac{1}{1 + \alpha^{q^{i+1}(q^j-1)}} \right)$$

$$= \sum_{j=1}^{m-1} \left(\frac{1}{1 + \alpha^{q(q^j-1)}} + \frac{1}{1 + \alpha^{q^{m+1-j}(q^j-1)}} \right)$$

Si ponemos $\beta = \alpha^q$, $I = m - J$ tenemos

$$\mathrm{Tr}(D(f)) = \sum_{j=1}^{m-1} \frac{1}{1 + \beta^{(q^j-1)}} + \sum_{I=1}^{m-1} \frac{1}{1 + \beta^{q^n - q^I}}$$

$$= \sum_{j=1}^{m-1} \frac{\beta}{\beta + \beta^{q^j}} + \sum_{I=1}^{m-1} \frac{\beta^{q^I}}{\beta^{q^m} + \beta^{q^I}}$$

Como $\beta^{q^m} = \beta$, tenemos:

$$\mathrm{Tr}(D(f)) = \sum_{j=1}^{m-1} 1 = m - 1$$

en un cuerpo de característica dos, luego se cumple el teorema (4.4).

(4.7) Lema: Si $f(x)$ y $g(x)$ son polinomios relativamente primos sobre $GF(2^n)$, entonces:

$$Tr(D(fg)) = Tr(D(f)) + Tr(D(g))$$

Demostración: Sean $\alpha_1, \ldots, \alpha_n$ raíces de $f(x)$ y $\alpha_{m+1}, \ldots, \alpha_{m+k}$ raíces de $g(x)$, entonces poniendo:

$$\sum_{1\le i<j\le m+k} \Sigma = \sum_{1\le i<j\le m} \Sigma + \sum_{m+1\le i<j\le m+k} \Sigma + \sum_{i=1}^{m+k} \sum_{j=m+1} \Sigma$$

en (4.5) se obtiene:

$$Tr(D(fg)) = Tr(D(f)) + Tr(D(g)) + \sum_{i=1}^{m} \sum_{j=m=1}^{m+k} \left[\frac{1}{1+\alpha_j/\alpha_i} + \frac{1}{1+(\alpha_j/\alpha_i)^q} \right]$$

Lūego (4.7) es equivalente a:

$$\sum_{i=1}^{m} \sum_{m+1}^{k} \frac{1}{1 + \alpha_j/\alpha_i} = \sum_{i=1}^{m} \sum_{j=m+1}^{k} \frac{1}{1 + (\alpha_j/\alpha_i)^q}$$

Obtendremos la igualdad anterior calculando ambos lados y demostrando que son iguales a:

$$\sum_{i=1}^{m} \sum_{j=m+1}^{k} \frac{1}{1 + \alpha_j^q/\alpha_i}$$

Como $\alpha_{m+1}, \ldots, \alpha_{m+k}$ son un sistema completo de conjugados se tiene que $\alpha_{m+1}^q, \ldots, \alpha_{m+k}^q$ son una permutación de $\alpha_{m+1}, \ldots, \alpha_{m+k}$, luego para todo i se tiene:

$$\sum_{j=m+1}^{k} \frac{1}{1 + \alpha_j^q/\alpha_i} = \sum_{j=m+1}^{k} \frac{1}{1 + \alpha_j/\alpha_i}$$

Utilizando el mismo argumento para $\alpha_1, \ldots, \alpha_m$ se tiene:

$$\sum_{i=1}^{m} \frac{1}{1 + \alpha_j^q/\alpha_i^q} = \sum_{i=1}^{m} \frac{1}{1 + \alpha_j^q/\alpha_i}$$

Esto demuestra el lema.

Daremos ahora la demostración del teorema (4.4).

Demostración (4.4): Sea $f(x) = \prod_{i=1}^{r} f^{(i)}(x)$, donde cada $f^{(i)}(x)$ es irreducible sobre $GF(2^n)$. Entonces en $GF(2)$ se tiene:

$$\begin{aligned} Tr(D(f)) &= \sum_{i=1}^{r} Tr(D(f^{(i)})) \qquad \text{por (4.7)} \\ &= \sum_{i=1}^{r} (\text{Deg } f^{(i)} - 1) \\ &= \text{Deg } f - r \ . \end{aligned}$$

Luego se tiene (4.4).

En el caso de característica impar, existe un teorema (Stikelberger) para determinar la paridad de la cantidad de factores irreducibles que descomponen a un polinomio $f(x)$. En este caso se utiliza la discriminante usual $\Delta(f(x))$.

Enunciaremos solamente el teorema, para la demostración ver $[Be]_1$.

(4.8) Teorema (Stikelberger): Sea q potencia de un primo $p \neq 2$. Sea $f(x)$ polinomio mónico de grado m sobre $GF(q)$ con discriminante $\Delta(f) \neq 0$. Sea r el número de factores irreducibles de $f(x)$ sobre $GF(q)$. Entonces $r \equiv m \pmod 2$ si y sólo si $\Delta(f)$ es un cuadrado en $GF(q)$.

Veamos ahora una aplicación de (4.4) para estudiar el caso de un trinomio:

Sea $f(x) = x^n + ax^k + b \in GF(2^m)[x]$ polinomio separable que es un producto de α factores irreducibles sobre $GF(2^m)$. Utilizando (4.4) estudiaremos la paridad de α. Para esto debemos calcular $Tr(D(f))$ en los siguientes casos:

I) n impar, k par.

(i) $K > 2$.

(a) Si $n \equiv \pm 1 \pmod 8$ $\quad D(f(x)) = 0$

Luego $\alpha \equiv m \pmod 2$ de modo que resulta: α impar

(b) Si $n \equiv \pm 3 \pmod 8$ entonces hay que distinguir los casos siguientes: (1) m par: se tiene $D(f(x)) = 0$ lo que implica que α es impar

(2) m impar: Se tiene $D(f(x)) \neq 0$ Luego $\alpha \not\equiv n \pmod 2$, es decir α es par.

(ii) $K = 2$

(a) Si $n \equiv \pm 1 \pmod 8$, entonces:

$Tr(D(f(x))) = 0$ si y sólo si (por teorema 90 de Hilbert) existe $\beta \in GF(2^m)$ con $D(f(x)) = \beta^2 + \beta$.

Luego α es impar equivale a $(\frac{a}{b})^{r/d} b^2 \in p(GF(2^m))$ si y sólo si $D(f(x)) \equiv 0 (\text{mod } p(GF(2^m))$.

(b) $n \equiv \pm 3 (\text{mod } 8)$ entonces hay que distinguir los casos:

(1) m es par: estamos entonces en (a)

(2) m es impar: utilizando el mismo argumento anterior tenemos:

α es impar si y sólo si $Tr(D(f(x))) = 0$ si y sólo si $1 + (\frac{a}{b})^{n/d} b^2 \in p(GF(2^m))$, si y sólo si $D(f(x)) \equiv 0 (\text{mod } p(GF(2^m))$.

II) m impar, k impar:

(i) $N > 2$.

(a) $(n - k)k \equiv \pm 1 (\text{mod } 8)$.

$Tr(D(f(x)) = 0$ luego $\alpha \equiv n (\text{mod } 2)$ es decir α es par.

(b) $(n - k)k \equiv \pm 3 (\text{mod } 8)$. Debemos nuevamente distinguir:

(1) m par: se reduce al caso (a) , es decir α es par

(2) m impar: $Tr(D(f(x)) = 1 \neq 0$, es decir $\alpha \not\equiv n (\text{mod } 2)$

Luego α es impar.

(ii) $N = 2$.

(a) $(n - k)k \equiv \pm 1 \pmod 8$, entonces se tiene

$Tr(D(f(x)) = 0$ si y sólo si existe $\gamma \in GF(2^m)$ con $D(f(x)) = \gamma^2 + \gamma$ (90 Hilbert), es decir α es par si y sólo si $\frac{b^{2-k/d}}{a^2} \in p(GF(2^m))$ si y sólo si $D(f(x)) \equiv 0 \pmod{p(GF(2^m))}$.

(b) $(n - k)k \equiv \pm 3 \pmod 8$ tenemos, entonces, los casos siguientes:

(1) m es par: Se reduce al caso (a).

(2) m es impar: Por el mismo argumento, α es par si y sólo si $1 + \frac{b^{2-k/d}}{a^2} \in p(GF(2^m))$ si y sólo si $D(f(x)) \equiv 0 \pmod{p(GF(2^m))}$.

III) n impar, k impar:

(i) $N - K > 2$, entonces si:

(a) $n \equiv \pm 1 \pmod 8$

$Tr(D(f(x)) = 0$ luego $\alpha \equiv m \pmod 2$ es decir α es impar

(b) $n \equiv \pm 3 \pmod 8$. Hay que distinguir:

(1) m par: se reduce a (a) luego α es impar

(2) m impar. Entonces $Tr(D(f(x)) \neq 0$ luego α es par

(ii) $N - K = 2$. Tenemos los siguientes casos:

(a) $n \equiv \pm 1 \pmod 8$ y $(n - k) \equiv 0 \pmod 4$

$Tr(D(f(x)) = 0$ luego α es impar

(b) $n \equiv \pm 3 \pmod 8$ y $(r - k) \equiv 0 \pmod 4$. Entonces hay que distinguir:

(1) m es par: $Tr(D(f(x)) = 0$. Luego α es impar

(2) m es impar: $Tr(D(f(x)) \neq 0$. Luego α es par.

(c) Si $n \equiv \pm 1 (\text{mod } 8)$, $(r - k) \equiv 1 (\text{mod } 4)$, entonces por teorema 90 de Hilbert: α es impar si y sólo si $Tr(D(f(x)) = 0$ si y sólo si existe $\delta \in GF(2^m)$ con $\frac{a^{2\ell+1}}{b^2} = \delta^2 + \delta \in p(GF(2^m))$, si y sólo si $D(f(x)) \equiv 0 (\text{mod } (GF(2^m))$.

(d) Si $n \equiv \pm 3 (\text{mod } 8)$ y $(n - k) \equiv 1 (\text{mod } 4)$. Entonces nuevamente debemos distinguir:

(1) m par: $D(f(x)) = \frac{a^{2\ell+1}}{b^2}$ y se utiliza el mismo argumento de (c).

(2) m impar: por el mismo argumento se tiene α es impar si y sólo si $1 + \frac{a^{2\ell+1}}{b^2} \in p(GF(2^m))$ si y sólo si $D(f(x)) \equiv 0 (\text{mod } p(GF(2^m))$

Resumiendo estos resultados podemos formular, entonces el siguiente resultado:

(4.8) Teorema: Sea $f(x) = x^n + ax^k + b$ polinomio separable que se descompone en α factores irreducibles sobre $GF(2^m)$. Sea $d = (n,k)$; $n = Nd$; $k = Kd$, entonces α es par si y sólo si se tiene alguno de los siguientes casos:

I) n impar, k par:

Si $K > 2$

$n \equiv \pm 3 \pmod 8$, m impar

Si $K = 2$,

$$n \equiv \begin{cases} \pm 1 \pmod 8 , & \left(\frac{a}{b}\right)^{n/d} b^2 \notin p(GF(2^m)) , \quad m \text{ cualquiera} \\ \pm 3 \pmod 8 , & \left(\frac{a}{b}\right)^{n/d} b^2 \notin p(GF(2^m)) , \quad m \text{ par} \\ \pm 3 \pmod 8 , & 1 + \left(\frac{a}{b}\right)^{n/d} b^2 \notin p(GF(2^m)) , \quad m \text{ impar} \end{cases}$$

II) n par, k impar.

Si $N > 2$

$$(n - k)k \equiv \begin{cases} \pm 1 \pmod 8 , & m \text{ cualquiera} \\ \pm 3 \pmod 8 , & m \text{ par} \end{cases}$$

Si $N = 2$

$$(n - k)k \equiv \begin{cases} \pm 3 , \ \pm 1 \pmod 8 , \ \frac{b^{2-k/d}}{a^2} \in p(GF(2^m)) , & m \text{ cualquiera} \\ \pm 3 \pmod 8 , \ \frac{1 + b^{2-k/d}}{a^2} \in p(GF(2^m)) , & m \text{ impar} \end{cases}$$

III) m impar, k impar

Si $N - K > 2$

$n \equiv \pm 3 \pmod 8$, m impar

Si $N - K = 2$

$$(n-k) \equiv \begin{cases} 0 \pmod 4 \ , \ n \equiv \pm 3 \pmod 8 \ , \ m \text{ impar} \\ 1 \pmod 4 \ , \ n \equiv \pm 1 \pmod 8 \ , \ \frac{a^N}{b^2} \notin p(GF(2^m)) \ , \ m \text{ cualquiera} \\ 1 \pmod 4 \ , \ n \equiv \pm 3 \pmod 8 \ , \ \frac{a^N}{b^2} \notin p(GF(2^m)) \ , \ m \text{ par} \\ 1 \pmod 4 \ , \ n \equiv \pm 3 \pmod 8 \ , \ 1 + \frac{a^N}{b^2} \notin p(GF(2^m)) \ , \ m \text{ impar} \end{cases}$$

En el teorema anterior, el caso n impar, k impar se puede reducir al caso n impar, k par haciendo el siguiente cambio de variable:

$$x^n + ax^k + b = y^{-n}b(y^n + a/by^{n-k} + 1/b)$$

donde $y = \frac{1}{x}$.

Se comprueba fácilmente que la paridad de la cantidad de factores irreducibles de $y^n + a/by^{n-k} + 1/b$ sobre $GF(2^m)$ coincide con lo de $x^n + ax^k + b$.

De este teorema se obtiene como corolario el resultado de Berlekamp:

(4.9) Corolario: Si n y k no son simultáneamente pares entonces $x^n + x^k + 1$ tiene una cantidad α , par de factores irreducibles sobre $GF(2)$ si y sólo si tiene alguno de los siguientes casos:

1) n par, k impar $nk/2 \equiv 0$ ó $1 \pmod 4$

2) n impar, k par $k/2n$, $n \equiv \pm 3 \pmod 8$

3) n impar, k par $k/2n$, $n \equiv \pm 1 \pmod 8$.

Demostración: Trataremos sólo los casos n par, k impar y n impar, k par, pués si n,k son impares utilizamos la reducción $(y^n + y^{n-k} + 1)$ donde $y = \frac{1}{x}$ que es equivalente al caso (2).

Como $m = 1$ es impar, por teorema (4.8) se tiene: α es par si y sólo si:

i) n impar, k par:

(a) $K > 2$ y $n \equiv \pm 3 \pmod 8$.

Pero si $K > 2$ se tiene $k / 2n$ pues K es par, es decir corresponde a las hipótesis del corolario.

(b) $K = 2$, y $n \equiv \pm 1 \pmod 8$.

Pero si $K = 2$, entonces $k/2n$ con lo cual nos reduciremos al caso (3) del cororlario.

ii) n par, k impar:

(a) $(n - k)k \equiv \pm 1 \pmod 8$

Pero si $(n - k)k \equiv \pm 1 \pmod 8$ se tiene $\frac{nk}{2} \equiv 0$ ó $1 \pmod 4$. Luego nos reducimos al caso (1).

(b) $(n - k)k \equiv \pm 3 \pmod 8$.

Pero si $(n - k)k \equiv \pm 3 \pmod 8$ nos podemos reducir nuevamente al caso (1).

A partir de estos casos se puede entonces dar una definición general del grupo de automorfismos propios:

(1.10) Definición:

$$O^+(M) = \{\sigma \in O(M) / \sigma(m) \in O^+(M(m)) \quad \forall\, m \in \text{máx}(A)\} .$$

Observación: $O^+(M) \lhd O(M)$.

Daremos ahora la última definición del párrafo:

(1.11) Definición: Sea (M,q) espacio cuadrático sobre un cuerpo k . Sea $\sigma : M \xrightarrow{\sim} M$ automorfismo. Entonces σ es una similitud si $q(\sigma(x)) = \lambda q(x)$, $\lambda \in k$, λ se llama norma de similitud de σ .

Observación: $O(M)$ es el grupo de similitudes de norma = 1.

Enunciaremos ahora su teorema que servirá posteriormente para aplicar los resultados de este párrafo: Para la demostración ver [Ba]$_1$.

(1.12) Teorema: Sea (M,q) espacio cuadrático sobre un anillo semi-local A . Denotemos por $\bar{M}$ la reducción de M módulo $m \in \text{Máx}(A)$. Entonces la aplicación

$$f_r : O^+(M) \to O^+(\bar{M})$$

es epiyectiva.

§ 2. Discriminantes de formas cuadráticas.

En este párrafo aplicaremos los resultados de (I. § 3) y (II. §1) con el fin de dar una demostración más simple del teorema 1.2 de [Ba]$_2$, en el caso de una rotación. Daremos primero una demostración del teorema en el caso de un cuerpo de característica $\neq 2$ ([Ed]) y reduciremos a este caso la demostración para un cuerpo de característica $= 2$. Denotaremos por $\Delta(k)$ al grupo k^*/k^{*2} si $2 \neq 0$ y $k/p(k)$ si $2 = 0$.

Enunciaremos primero el teorema general:

(2.1) Teorema: Sea (V,q) espacio cuadrático sobre un cuerpo k. Sea $\sigma \in O(V)$ un automorfismo con polinomio característico $P_\sigma(x)$ separable sobre k si $2 \neq 0$ supongamos $n = 2m$ y σ propio. Entonces en $\Delta(k)$ se tiene:

$$(-1)^{\frac{n(n-1)}{2}} (\det q) = \Delta(P_\sigma(x)) \quad \text{si } 2 \neq 0$$

$$\text{Arf } q = D(P_\sigma(x)) \quad \text{si } 2 = 0$$

Supongamos primero car $k \neq 2$. Entonces debemos demostrar:

$$d(q) = (-1)^{\frac{n(n-1)}{2}} \det q = \Delta(P_\sigma(x))$$

Sea $P_\sigma(x)$ el polinomio característico de σ. Entonces se comprueba fácilmente que $P_\sigma(x)$ es simétrico (Ver [Ba]$_2$). Luego $P_\sigma(x)$ es de la forma:

$$P_\sigma(x) = x^n - a_1x^{n-1} + \ldots + a_2x^2 - a_1x + 1 \ ;$$

donde $m = 2m$. Dividiendo $P_\sigma(x)$ por $x^m = x^{n/2}$

$$\frac{P_\sigma(x)}{x^m} = \left(x^m + \frac{1}{x^m}\right) - a_1\left(x^{m-1} + \frac{1}{x^{m-1}}\right) + \ldots + (-1)^m a_m$$

pongamos $z = x + \frac{1}{x}$. Entonces $\frac{P_\sigma(x)}{x^m}$ puede ser escrito como un polinomio irreducible de grado m en z . (Ver [Di]).

$$h(z) = z^m + b_1z^{m-1} + \ldots + b_m$$

Sean $\alpha_1, \ldots, \alpha_m$ las raíces distintas de $h(z)$ en $\bar{k}$, clausura algebraica de k

$$h(z) = (z - \alpha_1) \ldots (z - \alpha_m)$$

Si $z = -2$, $x = -1$ se tiene:

$$h(-2) = \frac{f(-1)}{(-1)^m}$$

es decir

$$(-2 - \alpha_1) \ldots (-2 - \alpha_m) = \frac{[(-1)^n - a_1(-1)^{n-1} + \ldots + 1]}{(-1)^m}$$

es decir

$$(2 + \alpha_1) \ldots (2 + \alpha_m) = 2 + 2a_1 + \ldots 2a_{m-1} + a_m$$

De la misma manera, poniendo $z = 2$ tenemos

$$h(2) = f(1)$$

y $\quad (2 - \alpha_1) \ldots (2 - \alpha_m) = 2 - 2a_1 + \ldots + (-1)^m a_m$

Combinando ambas ecuaciones

$$(4-\alpha_1^2) \ldots (4-\alpha_m)^2 = (2+2a_1 + \ldots + a_m)(2-a_1 + \ldots + (-1)^m a_m) \quad (2.1.3)$$

Utilizando el teorema (2.4) del capítulo I y aplicándolo a los polinomios $P_{\sigma_i}(x) = x^2 - \alpha_i x + 1$, deducimos:

$$\Delta(P_{\sigma_i}(x)) \cdot P_{\sigma_j}(x)) = (\alpha_i^2 - 4)(\alpha_j^2 - 4) R(P_{\sigma_i}(x), P_{\sigma_j}(x))^2$$

Pero es fácil demostrar que:

$$R(P_{\sigma_i}(x), P_{\sigma_j}(x)) = (\alpha_i - \alpha_j)^2 ,$$

de modo que

$$\Delta(P_\sigma(x)) = \Delta[(x^2 - \alpha_1 x + 1) \ldots (x^2 - \alpha_m x + 1)]$$

$$= (\alpha_1^2 - 4) \ldots (\alpha_m^2 - 4) \prod_{i<j} (\alpha_i - \alpha_j)^2$$

$$= (-1)^m (4 - \alpha_1^2) \ldots (4 - \alpha_m^2)(\Delta(h(z)))^2$$

Estudiaremos ahora la expresión de la derecha de (2.1.1). Por un resultado de Zassenhauss (ver [Z]) se sabe que la norma espinorial de una rotación σ con polinomio característico $x^n - a_1 x^{n-1} + \ldots - a_1 x + 1$ es:

$$S_n(\sigma) = 2 + 2a_1 + \ldots + 2a_{n-1} + a_m (\text{mod } k^{*2}) \quad (2.1.2)$$

donde $n = 2m$. Nuevamente por un resultado de Zassenhauss ([Z]) se sabe que la norma espinorial de -1_V es la determinante de (V,q) , es decir:

$$S_m(-1_V) = \det(q) \qquad (2.1.3)$$

Escribiendo σ en una base conveniente se obtiene para σ una matriz

$$S = \begin{vmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ & & & & & \\ 0 & \ldots & \ldots & \ldots & 0 & 1 \\ -1 & a_1 & -a_2 & \ldots & -a_2 & a_1 \end{vmatrix}$$

Sea τ la rotación dada por la siguiente matriz con respecto a la misma base:

$$T = \begin{vmatrix} -a_1 & a_2 & -a_3 & \ldots & -a_1 & 1 \\ -1 & 0 & \ldots & \ldots & \ldots & 0 \\ 0 & -1 & 0 & 0 & \ldots & 0 \\ & & & & & \\ 0 & 0 & 0 & \ldots & -1 & 0 \end{vmatrix}$$

Entonces $\sigma \cdot \tau = 1_V$ y el polinomio característico de τ es:

$$g(x) = x^n + a_1 x^{m-1} + \ldots + a_2 x^2 + a_1 x + 1$$

Luego por (2.1.2):

$$S_n(\sigma) = (2 + 2a_1 + \ldots + a_m) (\text{mod } k^{*2})$$

$$S_n(\tau) = (2 - 2a_1 + \ldots + (-1)^m a_m) (\text{mod } k^{*2})$$

Luego por (2.1.3):

$$\begin{aligned} \det(q) &= S_n(-1_V) \\ &= S_n(\sigma) S_n(\tau) \\ &= (2+a_1 + \ldots + a_m)(2-2a_1 + \ldots + (-1)^m a_m) (\text{mod } k^{*2}) \\ &= (4 - \alpha_1^2) \ldots (4 - \alpha_m^2) (\text{mod } k^{*2}) \end{aligned}$$

Luego

$$\Delta(P_\sigma(x)) = (-1)^m (4 - \alpha_1^2) \ldots (4 - \alpha_m^2) (\text{mod } k^{*2})$$

$$= (-1)^m \det(q) = (-1)^{\frac{n(n-1)}{2}} \det(q)$$

Reduciremos ahora, utilizando los resultados de los párrafos § 3, capítulo I y § 1, capítulo II el caso car k = 2 , al caso car $\neq$ 2 . Nuestra demostración es solo aplicable a automorfismos propios.

Supongamos $\sigma \in O^+(V)$, automorfismo propio. Sea A anillo de valuación discreta, completo con cuerpo residual k , uniformizante = 2 y car A = 0 (ver I, § 3) . Llamemos

$\bar{q}$ a la forma cuadrática definida sobre V y sea M un A-módulo libre con $\dim_A M = \dim_k V$ y tal que $M \otimes_A k = V$.

Sea q forma cuadrática definida en M y tal que su reducción módulo 2 coincide con $\bar{q}$. Tenemos entonces un módulo cuadrático (M,q) sobre A cuyo espacio cuadrático reducido es $(V,\bar{q})$.

Sea $K = \mathrm{Quot}(A)$ y consideremos el espacio cuadrático

$$(M_K, q_K) \supseteq (M,q) \quad ; \quad M_K \otimes_K A = M \ .$$

Tomemos $\bar{\sigma}$ automorfismo propio de V , $\bar{\sigma} \in O^+(V)$. Entonces aplicando el teorema (1.12) se tiene: Existe $\sigma \in O^+(M)$ pre-imagen de $\bar{\sigma}$. Consideremos $\sigma \in \mathrm{Aut}_A(M,q)$ como un automorfismo σ_K del espacio cuadrático (M_K, q_K) extendiendo escalares. Sea $P_{\sigma_k}(x)$ el polinomio característico de σ_K sobre K . Entonces:

1) $P_{\sigma_K}(x)$ está definida sobre A .

2) $\Delta(P_{\sigma_K}(x)) \in A^*/A^{*2}$, más aún en $\in S/A^{*2}$.

Luego aplicando el teorema para el caso car $k \neq 2$ se tiene:

$$\Delta(P_{\sigma_K}(x)) = (-1)^{\frac{n(n-1)}{2}} \det(q_K)$$

Pero son todos elementos de A^*/A^{*2} , luego:

$$\Delta(P_{\sigma}(x)) = (-1)^{\frac{n(n-1)}{2}} \det(q) \quad \text{en} \quad A^*/A^{*2} \quad \text{pues}$$

$$A^*/A^{*2} \longrightarrow K^*/K^{*2} \quad \text{es inyectivo.}$$

Aplicando el epimorfismo γ (ver § 3, capítulo I) se obtiene por lema (1.8), capítulo II:

(2.1.4) $$\gamma(\Delta(P_\sigma(x)) = Arf(\overline{q})$$

para todo σ automorfismo propio.

Pero por lema (3.3), capítulo I , como $P_\sigma(x)$ es levantamiento de $P_{\overline{\sigma}}(x)$ pués σ es levantamiento de $\overline{\sigma}$ se obtiene la igualdad (2.1.4). Comparando las igualdades anteriores se deduce:

$$D(P_{\overline{\sigma}}(x)) = Arf(\overline{q})$$

APENDICE.

En el caso de cuerpos de característica 2, existe otra discriminante, introducida por Revoy en [Rev] para extensiones finitas y separables que corresponden en el caso $2 \neq 0$ a la discriminante de la forma bilineal $(x,y) \to Tr(x \cdot y)$, asociada a una extensión separable L/K.

Utilizando algunos resultados anteriores, daremos, en este Apéndice, la demostración de Wadsworth para una conjetura de Revoy que relaciona la discriminante de Revoy con la discriminante de Berlekamp.

Sea L/F extensión finita y separable, car $F = 2$. Sea N la clausura normal de L sobre F. Sobre L definimos la función $Q_r : L \to F$ como: $Q_r(a) = \sum_{1 \leq i < j \leq n} \tau_i(a)\tau_j(a)$ donde τ_i son los distintos F-automorfismos de L en N. Es fácil demostrar que $Q_r(a) \in F$ para todo $a \in L$. Además se comprueba que Q_r es forma cuadrática sobre F con forma bilineal asociada:

$$B_{Q_r}(x,y) = Tr(x) \cdot Tr(y) - Tr(x \cdot y)$$

donde $Tr : L \to F$ es la traza de L/F.

Observación: Si $[L : F]$ es par, entonces $[L,Q_r]$ es no singular.

Si $[L : F]$ es impar, entonces $[(\ker Tr),Q_r]$ es no singular. (ver [Re]).

Definición: Se define la discriminante de Revoy de L/F como:

$$\rho_{L/F} := Arf(Q_r) \in F/p(F)$$

donde Q_r denota la forma (L,Q_r) si $[L : F]$ es par y $((\ker Tr),Q_r)$ si $[L : F]$ es impar. Denotaremos por W al espacio vectorial de esta forma.

Por otro lado, al polinomio minimal de L/F (separable) $f(x)$ se le asocia la invariante de Berlekamp:

$$\beta_{L/F} := D(f(x)) \in F/p(F)$$

Wadsworth demostró el siguiente resultado que responde a una conjetura de Revoy.

Teorema: Sea L/F extensión finita y separable de F, car $F = 2$. Entonces

$$\rho_{L/F} = \begin{cases} \beta_{L/F} \text{ en } F/p(F) \text{ si } [L : F] \equiv 0,1,2 \text{ ó } 7 \pmod 8 \\ \beta_{L/F} + 1 \text{ en } F/p(F) \text{ si } [L : F] \equiv 3,4,5 \text{ ó } 6 \pmod 8 \end{cases}$$

Demostración: Utilizaremos el método de levantamiento, introducido en § 3 del Capítulo I, para reducirnos al caso de característica 0.

Sea N cuerpo de descomposición de $f(x)$ y $\overline{\alpha_1}, \ldots, \overline{\alpha_n}$ las raíces de $f(x)$, $f(x) = \prod_{i=1}^{n} (x - \overline{\alpha_i})$ en $N[x]$.

Sea $L = F(\alpha)$, $\overline{\alpha}$ una raíz de f. Sea $V \longrightarrow F'$, como en § 3, Capítulo I, anillo de valuación discreta, car $V = 0$, $V/2V = F$ y $F' = \mathrm{Quot}(V)$.

Sea $g(x) \in V[x]$ levantamiento mónico de $f(x)$ y N' cuerpo de descomposición de $g(x)$. Tenemos entonces

$$g(t) = \prod_{i=1}^{n} (t - \alpha_i)$$

α_i raíces de g en N'.

Entonces N' tiene valuación discreta, que extiende la de F' y se tiene, $\alpha_i \overset{\text{red}}{\longmapsto} \overline{\alpha_i}$. Sea $L' = F'(\alpha)$ con $\alpha \overset{\text{red}}{\longmapsto} \overline{\alpha}$. Sea B anillo de valuación de N'. Tenemos entonces el siguiente diagrama.

$$\begin{array}{ccccc}
N' & \text{———} & B & \longrightarrow\!\!\!\!\rightarrow & N = F(\overline{\alpha_1}, \ldots, \overline{\alpha_n}) \\
\uparrow & & \uparrow & & | \\
L' = F(\alpha) & \text{———} & B \cap L' = V_L & \longrightarrow\!\!\!\!\rightarrow & L = F(\overline{\alpha}) \\
\uparrow & & \uparrow & & | \\
F' & \text{———} & V & \longrightarrow\!\!\!\!\rightarrow & F
\end{array}$$

Se tiene que $L' = F(\alpha)$ está definido por el polinomio $g(t)$ y la discriminante de L'/F' es:

$$\Delta_{L'/F'} = \det(Q) \pmod{F'^{*2}}$$

Donde $Q : L' \to F'$ es la forma cuadrática $Q(x) = \frac{1}{2} \mathrm{Tr}_{L'/F'}(x^2)$ con forma bilineal simétrica asociado $B_Q(x,y) = \mathrm{Tr}_{L'/F'}(x \cdot y)$. Sea $W = V_L$ si $|L : F|$ es par y $W = V_L \cap |\ker \mathrm{Tr}_{L'/F'}|$ si $|L : F|$ es impar. W es V-módulo libre con $W \otimes F = \overline{W}$ y donde está definida la forma cuadrática siguiente:

$$Q'_r(x) = \sum_{1 \leq i < j \leq n} \tau'_i(x)\tau'_j(x) = \frac{1}{2} \left| (\mathrm{Tr}_{L'/F'}(x))^2 - \mathrm{Tr}_{L'/F'}(x^2) \right|$$

<u>Observación</u>: $\overline{Q'_r} = Q_r$ y $B_{Q'_r}(x,y) = \mathrm{Tr}_{L'/F'}(x) \cdot \mathrm{Tr}_{L'/F'}(y) - \mathrm{Tr}(x \cdot y)$.

Como $V^*/V^{*2} \longrightarrow F'^*/F'^{*2}$ entonces, extendiendo escalares, podemos, sin restricción, considerar a Q'_r y Q como formas en WF' y L' respectivamente.

Supongamos que n es par. Entonces $W = V_L$ y por lo tanto $WF' = L'$. Sea $L_o = \ker(\mathrm{Tr})$, entonces la descomposición $L' = F' \oplus L_o$ es una suma ortogonal para Q'_r es Q .

Más aún, sobre L_o Q'_r coincide con $-Q$. Tenemos entonces en F'^*/F'^{*2}

$$\det Q\Big|_{L_o} = (\det Q)_{(\det Q/F')} = \Delta_{L'/F'}/n$$

Luego en F'^*/F'^{*2} , como $\det Q'_r\big|_{F'} = n^2 - n$, se tiene:

$$\det Q'_r = (n^2 - n)\cdot\det(Q'_r\big|_{L_o}) = (n^2 - n)\det(-Q\big|_{L_o})$$

$$= -(n^2 - n)\Delta_{L'/F'}{}_n = (1 - n)\Delta_{L'/F'}$$

Si n es impar, entonces $WF' = L_o$ luego en F'^*/F'^{*2}

$$\det(Q'_r) = \det(-Q\big|_{L_o})$$

$$= (\Delta_{L'/F'})_n \equiv n\,\Delta_{L'/F'}$$

Aplicando el epimorfismo γ introducido en §3, Capítulo I y los lemas (3.3) y (II;(1.7) se tiene:

$$\rho_{L/F} := \mathrm{Arf}(Q_r) = \gamma(\det Q'_r) = \begin{cases} \gamma(1 - n) + \gamma(\Delta_{L'/F'}) \\ \\ \gamma(n) + \gamma(\Delta_{L'/F'}) \end{cases}$$

$$= \begin{cases} \gamma(1 - n) + \beta_{L/F} & \text{si } n \text{ par} \\ \\ \gamma(n) + \beta_{L/F} & \text{si } n \text{ es impar} \end{cases}$$

Claramente $\gamma(k)$ está definida para todo entero impar k y dependiendo de las clases módulo 8 pués: Sup k entero impar, entonces:

$$k = 2t + 1 \quad , \quad t \in \mathbb{Z}$$

Si $t \equiv 0 \pmod 2$: $k = 4s + 1$, $s \in \mathbb{Z}$

Luego: $\gamma(k) = \gamma(1 + 4s) = \overline{s} \pmod 2$:

Si $s \equiv 0 \pmod 2$, entonces $k \equiv 1 \pmod 8$

Si $s \equiv 1 \pmod 2$, entonces $k \equiv 5 \pmod 8$

Si $t \equiv 1 \pmod 2$: $k = 4t + 3$

$$= -1 + 4(t + 1)$$

Luego: $\gamma(k) = (\overline{t + 1}) \pmod 2$

Si $t \equiv 0 \pmod 2$, $k \equiv 3 \pmod 8$

Si $t \equiv 1 \pmod 2$, $k \equiv 7 \pmod 8$

Luego sólo depende de las clases módulo 8 . Más aún, tenemos:

$$\gamma(7) = \gamma(1) = 0 \quad \text{y} \quad \gamma(3) = \gamma(5) = 1 \ .$$

Luego se tiene el teorema.

R E F E R E N C I A S.

[Ba]$_1$ R. Baeza: Quadratic Forms over Semi-local Rings. Springer-Verlag. Lecture Notes in Math. N° 655 (1978).

[Ba]$_2$ R. Baeza: Discriminants of Polynomials and of Quadratic Forms. Journal of Algebra, Vol. 72; N° 1 Septiembre (1981).

[Be]$_1$ E.R. Berlekamp: Algebraic Coding Theory. Mc. Graw-Hill, New York (1968).

[Be]$_2$ E.R. Berlekamp: An Analog to the Discriminant over Fields of Characteristic two. Journal of Algebra 38, 315-317 (1976).

[CP] P.E. Conner y R. Perlis: The Witt Class of a Trace Form. Louisiana State University. Baton Rouge (1982) Pre-print.

[Ed] B.H. Edwards: Rotations and Discriminants of Quadratic Forms. Linear and Multi-linear Algebra 8, (1980). 241-246.

[Gr] M.J. Greenberg: Lecture on Forms in Many Variables. W.A. Benjamin (1969).

[La] S. Lang: Algebra. Addison Wesley (1965).

[Rev] P. Revoy: Remarques sur la Norme Trace. Linear and Multi-linear Algebra. Vol. 10, pp. 223-233 (1981).

[Se] J.P. Serre: Corps Locaux. Publications de l'Institut de Mathématique de l'Université de Nancaps VIII. Ed. Hermann (1962).

[VdW] Van der Waerden: Modern Algebra. Frederick Unpar Publishing Co. New York (1953).

[Wads] A. Wadsworth: Discriminants in Characteristic 2. (9 Sept, 1982) por publicar en Linear and Multi-linear Algebra.

[Z] H. Zassenhaus: On the Spinor Norm. Archiv. der Math. Vol. XIII (1962), pp. 439-451.

CAPITULO II. DISCRIMINANTE DE FORMAS CUADRATICAS.

§ 1. Relaciones entre la discriminante de Berlekamp y formas cuadráticas.

En este párrafo se introducirán algunas nociones básicas de la teoría de formas cuadráticas sobre anillos semi-locales que servirán para demostrar una relación entre la discriminante de Berlekamp y la invariante de Arf de una forma cuadrática. Esta relación servirá posteriormente, en § 2 para dar una demostración más elemental del resultado del trabajo Discriminants of Polynomials and Quadratic Forms [Ba]$_2$ para el caso car k = 2 .

(1.1) Definición: Sea A un anillo conmutativo con 1, M A-módulo proyectivo finitamente generado. Una forma bilineal $B : M \times M \to A$ se dice simétrica si $B(x,y) = B(y,x)$ para todo $x,y \in M$.

Sea (M,B) módulo bilineal sobre A . Para todo $x \in M$ se define:

$d_B(x) \in \mathrm{Hom}(M,A)$ poniendo: $d_B(x)(y) = B(x,y)$ para todo $y \in M$.

Luego tenemos una aplicación A-lineal $d_B : M \to \mathrm{Hom}(M,A)$. El módulo bilineal (M,B) se llama no singular si d_b es

un isomorfismo.

Observación: Sea $M = Ae_1 \oplus \ldots \oplus Ae_n$ A-módulo libre de dimensión n, B forma bilineal simétrica sobre M. Entonces la forma B está definida por la matriz (B_{ij}) donde $B_{ij} = B(e_i, e_j)$.

El módulo bilineal (M,B) es no singular si $\det(B_{ij}) \in A^*$.

(1.2) Definición: Sea $m \in \text{máx}(A)$, (M,b) A-módulo bilineal, entonces se define la reducción de (M,B) módulo m, como la forma bilineal sobre A/m, $(M(m),B(m))$, donde $M(m) = M/_{mM}$ y $B(m) = M(m) \times M(m) \to A/m$ está definida por $B(m)(\bar{x},\bar{y}) = \overline{B(x,y)}$ para todo $\bar{x},\bar{y} \in M(m)$.

(1.3) Definición: Sea M A-módulo proyectivo finitamente generado. Se define una forma cuadrática en M como una aplicación: $q : M \to A$ con las siguientes propiedades:

(1) $\quad q(\lambda x) = \lambda^2 q(x) \quad \forall\, x \in M, \quad \lambda \in A$

(2) $\quad B_q(x,y) = q(x+y) - q(x) - q(y)$ define una forma bilineal $B_q : M \times M \to A$.

El par (M,q) se llama módulo cuadrático sobre A y (M,B_q) es el módulo bilineal asociado. Si (M,B_q) es no singular, entonces (M,q) se llama no singular o espacio cuadrático.

Análogamente al caso bilineal, se define para $m \in \text{Máx}(A)$

la reducción $(M(m),q(m))$ de un módulo cuadrático.

(1.4) Proposición: Para todo módulo cuadrático son equivalentes:

(1) (M,q) es no singular.

(2) $(M(m),q(m))$ es no singular para todo $m \in Máx(A)$.

(1.5) Observación: Si car $A = 2$ se tiene $B_q(x,x) = 2q(x,x) = 0$ para toda forma cuadrática q , luego b_q es alternada.

Si q es no degenerada se tiene dim M es par y M tiene base simpléctica $x_1, \ldots, x_e, y_1, \ldots, y_e$ es decir $B_q(x_i,x_j) = 0 = B_q(y_i,y_j)$ para todo i,j y $B_q(x_i,y_j) = \delta_{ij}$.

(1.6) Definición: Sea V F-espacio vectorial, supongamos car$(F) = 2$ y q forma cuadrática no degenerada sobre V . Sea $\{x_1, \ldots, x_e, y_1, \ldots, y_e\}$ base simpléctica de V . Se define la invariante de Arf de q en $F/p(F)$ como:

$$Arf(q) = \sum_{i=1}^{e} q(x_i)q(y_i) \pmod{p(F)}$$

Esto es una invariante de (M,q) , es decir si $\{x_i', y_i'\}$ es otra base simpléctica de (M,q) , entonces $\Sigma q(x_i)q(y_i) \equiv \Sigma q(x_i')q(y_i') \bmod p(P)$. Para la demostración ver [Ba]$_1$.

La invariante de Arf de una forma cuadrática sobre un cuerpo de característica 2 se puede reducir al cálculo de la

discriminante usual de una forma cuadrática sobre un cuerpo de característica 0 usando el método introducido en (I, § 3) de la siguiente manera:

Sea F cuerpo, $car(F) = 2$. Sea V , como en (I, § 3), anillo de valuación discreta, con cuerpo residual F , uniformizante 2 y $car\ V = 0$.

Sea M un V-módulo libre de rango $m < \infty$. Sea $q : M \to V$ forma cuadrática sobre M y sea $\overline{M} = M/2M$ un F-espacio vectorial y $\overline{q} : \overline{M} \to F$ la forma cuadrática reducida. La determinante del espacio cuadrático (M,q) sobre V está definida como la clase $\det(B_q(e_i,e_j) \bmod V^{*2}$ en V^*/V^{*2} donde $\{e_1, \ldots, e_n\}$ es una base cualquiera de M sobre V . Esta clase se denota por $\det(q)$. Se comprueba que $\det(q) \in S/V^{*2} < V^*/V^{*2}$ (ver demostración (1.7)).

El siguiente resultado de Wadsworth relaciona $\det(q)$ con la invariante de Arf de $(\overline{M},\overline{q})$.

(1.7) Lema: $\det q \in S/V^*$ y

$$\gamma(\det q) = Arf(\overline{q})$$

Demostración: Como $\overline{q}$ es no degenerada, existe base simpléctica $\overline{x}_1, \ldots, \overline{x}_e, \overline{y}_1, \ldots, \overline{y}_e$. Tomemos pre-imágenes x_i, y_i de $\overline{x}_i, \overline{y}_i$ en M , $i = 1, \ldots e$. Entonces $\{x_1,y_1, \ldots, x_e y_e\}$ es base de M con $B_q(x_i,x_j)$, $B_q(y_i,y_j) \in 2V$ y

$B_q(x_i , y_j) \in \delta_{ij} + 2V$ para todo i,j .

Usando técnicas de ortogonalización, podemos encontrar $x'_1,y'_1,\ldots,x'_e,y'_e$ con $x'_i \equiv x_i \pmod{2M}$, $y'_i \equiv y_i \pmod{2M}$, $B_q(x'_i,y'_i) = 1$ para todo i y si $i \neq j$, $B_q(x'_i,x'_j) = B_q(y'_i,y'_j) = B_q(x'_i,y'_j) = 0$.

La matriz B_q relativa a la base $x'_1,y'_1, \ldots, x'_e,y'_e$ es en bloques diagonales con el i-ésimo bloque de la forma:

$$\begin{pmatrix} 2q(x'_i) & 1 \\ 1 & 2q(y'_i) \end{pmatrix}$$

Se obtiene, entonces, $\det q = \prod_{i=1}^{e} 4(q(x'_i)q(y'_i) - 1) \in S/V^{*2}$ y aplicando el homomorfismo γ introducido en (I, § 3) tenemos:

$$\gamma(\det q) = \sum_{i=1}^{e} \gamma(4(q(x'_i)q(y'_i) - 1)$$

$$= \sum_{i=1}^{e} \overline{q(x'_i)q(y'_i)}$$

$$= \sum_{i=1}^{e} \bar{q}(\bar{x}_i) \cdot \bar{q}(\bar{y}_i)$$

$$= \mathrm{Arf}(\bar{q})$$

Introduciremos ahora otra definición relativa a formas cuadráticas:

(1.8) Definición: Sea (M,q) espacio cuadrático sobre un anillo A. Un automorfismo σ de (M,q) es un isomorfismo $\sigma : M \xrightarrow{\sim} M$ tal que $q(\sigma(x)) = q(x) \quad \forall\, x \in M$.

Denotaremos al grupo de automorfismos de (M,q) por $O(M)$. Este grupo se llama el grupo ortogonal de (M,q).

Sea (M,q) espacio cuadrático sobre un anillo semilocal A. Para $\sigma \in O(M)$ denotemos por $\sigma(m)$ la reducción módulo $m \in Máx(A)$. A continuación definiremos el grupo de automorfismos propios de (M,q) : $O^+(M)$. Con este fin, recordaremos las definiciones de O^+ para espacios cuadráticos sobre cuerpos, considerando las reducciones de (M,q) módulo los ideales maximales de A, tenemos los casos: Sea $m \in Máx(A)$

i) $car(A/m) \neq 2$. Entonces para todo $\sigma(m) \in O(M(m))$

$$[\det \sigma]^2 = 1 \quad \text{es decir} \quad \det \sigma = \pm 1$$

y

$$O^+(M(m)) = \{\sigma(m) \in O(M(m)) / \det\sigma = 1\}$$

ii) $car(A/m) = 2$. Entonces $\det\sigma = 1$ para todo $\sigma \in O(M)$. Luego el determinante no es una invariante importante para σ. En este caso se introduce una nueva invariante que se define de la siguiente manera:

El espacio $(M(m),q(m))$ tiene base $\{e_1, \ldots, e_n, f_1, \ldots, f_n\}$ con: $q(e_i) = a_i$, $q(f_i) = b_i$, $(e_i f_i) = 1$ y

$M(m) = \langle e_1, f_1 \rangle \perp \ldots \perp \langle e_n, f_n \rangle$ donde $\langle e_i, f_i \rangle = [a_i, b_i]$

Entonces todo $\sigma(m) \in 0(M(m))$ se define por:

$$\sigma(m)(e_i) = \sum_{j=1}^{m} (\alpha_{ij} e_j + \beta_{ij} f_j)$$

$$\sigma(m)(f_i) = \sum_{j=1}^{n} (\delta_{ij} e_j + \delta_{ij} f_j)$$

con $\alpha_{ij}, \ldots, \delta_{ij} \in A/m$.

Definimos entonces:

(1.9) Definición:

$$D(\sigma) = \sum_{i,j} (a_j \alpha_{ij} \gamma_{ij} + \beta_{ij} \gamma_{ij} + b_j \beta_{ij} \delta_{ij}) .$$

Este elemento de A/m es una invariante, es decir, independiente de la base $\{e_i, f_i\}$ y para todo $\sigma \in 0(M(m))$ se tiene:

$$D(\sigma)^2 + D(\sigma) = 0$$

Luego $D(\sigma) = 0$ ó 1

Entonces

$$0^+(M(m)) = \{\sigma \in (M(m))/D(\sigma) = 0\}$$