

UNIVERSITAT DE BÀRCELONA

FACULTAT DE MATEMÀTIQUES

**SOBRE EL NUMERO DE EXTENSIONES DE GRADO
DADO DE UN CUERPO LOCAL**

by

ARTUR TRAVESA I GRAU



PRE-PRINT N.º 42

MARÇ-1986

SOBRE EL NÚMERO DE EXTENSIONES DE GRADO DADO DE UN CUERPO LOCAL

Artur Travesa i Grau

Dept. d'Àlgebra i Fonaments. Fac. de Matemàtiques. Univ. de Barcelona

ABSTRACT.- In [1] and [4] M. Krasner and J.-P. Serre obtained, by two essentially different methods, formulas about the number of separable totally ramified extensions of given degree and discriminant of a local field. In this work we prove the equivalence between these two formulas, deducing the Krasner's ones from the Serre's ones. Moreover, we extend the Serre's formulas in order to include the not totally ramified case.

RESUMEN.- En [1] y [4] M. Krasner y J.-P. Serre obtuvieron, por métodos esencialmente distintos, fórmulas que dan el número de extensiones separables, totalmente ramificadas, y de grado y discriminante dados de un cuerpo local. En este trabajo se demuestra la equivalencia de ambas fórmulas, deduciendo las de Krasner a partir de las de Serre. Asimismo, se extienden las fórmulas de Serre a fin de incluir en ellas el caso no totalmente ramificado.

1. NOTACIONES.- Sea K un cuerpo local con cuerpo residual de q elementos y característica p . Sea A el anillo de la valoración y sea $\mathfrak{p}$ el ideal maximal de A . Normalizamos la valoración de K de manera que $v_K(\pi)=1$ para un parámetro uniformizante π de A . Sea K_s una clausura separable de K .

En todo lo que sigue L será una extensión finita de K , $L \subset K_s$; B , la clausura entera de A en L , y $\mathfrak{P}$, el ideal maximal de B . Los cuerpos residuales de K y L los denotaremos respectivamente por $\bar{K}$ y $\bar{L}$, y v_L será la valoración (normalizada) de L .

Dados números naturales n, e, c , con $n \geq 2$ y $e|n$, escribiremos:

$\Sigma(n, K)$ = conjunto de las extensiones de K , $L \subset K_s$, de grado $[L:K]=n$;

$\Sigma(n, e, K)$ = conjunto de las extensiones de K , $L \subset K_s$, de grado n y con índice de ramificación $e(\mathfrak{P}|\mathfrak{p})=e$;

$\Sigma(n, e, c, K)$ = conjunto de las extensiones de K , $L \subset K_s$, de grado n , índice de ramificación e , y diferente $D(L|K)=p^{e-1+c}$.

2. LAS CONDICIONES DE ÖRE.- Sea $L \in \Sigma(n, e, K)$. La diferente de L sobre K



puede escribirse en la forma

$$\mathcal{D}(L|K) = p^{e-1+c(L|K)},$$

donde $c = c(L|K)$ es un número natural que vale cero si y sólo si $p \nmid e$.

Se tiene, en general, el siguiente resultado:

LEMA (ÖRE). - $\Sigma(n, e, c, K) \neq \emptyset$ si y sólo si c satisface las condiciones:

$$(1) \quad e \cdot v_K(\ell) \leq c \leq e \cdot v_K(e),$$

donde ℓ es el único natural $1 \leq \ell \leq e$, con $c \equiv \ell \pmod{e}$.

Observaciones: 1.- En el caso equicaracterístico, si $p \mid e$ resulta que $v_K(e) = +\infty$; Entonces las condiciones (1) se reducen a $p \nmid c$. En efecto, si $p \mid c$ entonces $v_K(\ell) = +\infty$, de manera que $c = +\infty$, y $L|K$ no sería separable.

2.- En particular, se deduce de este lema que si $p \nmid e$, entonces $\Sigma(n, e, c, K) \neq \emptyset$ si y sólo si $c = 0$.

Demostración.- Descomponiendo la extensión $L|K$ en su parte no ramificada $K_0|K$ y su parte totalmente ramificada $L|K_0$, y puesto que $v_{K_0} = v_K$ podemos limitarnos al caso totalmente ramificado ($e=n$). En este caso, las condiciones de Öre se escriben en la forma:

$$(1') \quad n \cdot v_K(\ell) \leq c \leq n \cdot v_K(n),$$

donde $1 \leq \ell \leq n$ y $c \equiv \ell \pmod{n}$.

Sea $L \in \Sigma(n, n, c, K)$ y sea Π un uniformizante de B . Entonces Π satisface una ecuación de Eisenstein $f(\Pi) = 0$, donde

$$(2) \quad f(X) = a_0 + a_1 X + \dots + a_{n-1} X^{n-1} + X^n, \quad a_i \in p, \quad a_0 \in p \setminus p^2.$$

Además, $B = A[\Pi]$ y la diferente viene dada por ([5] Cap. III)

$$\mathcal{D}(L|K) = p^{v_L(f'(\Pi))}.$$

Pero $f'(\Pi) = n\Pi^{n-1} + \sum_{i=1}^{n-1} (n-i)a_{n-i}\Pi^{n-i-1}$, y las valoraciones de los sumandos son

$$n-1+v_L(n), \quad n-1-i+v_L(n-i)+v_L(a_{n-i}), \quad 1 \leq i \leq n-1.$$

Además, al ser $f'(\Pi) \neq 0$, alguna de ellas es finita. Puesto que $v_L = n \cdot v_K$ resulta que las que corresponden a sumandos no nulos son todas distintas (reducir módulo n) y, por lo tanto,

$$v_L(f'(\Pi)) = \inf_{1 \leq i \leq n-1} \{n-1+v_L(n); n-1-i+v_L(n-i)+v_L(a_{n-i})\}.$$

Esto nos dice que $v_L(f'(\Pi)) = n-1+c$ si y sólo si

1983

$$c = \inf_{1 \leq i \leq n-1} \{v_L(n), -i + v_L(n-i) + v_L(a_{n-i})\}.$$

Si $c \equiv 0 \pmod{n}$, entonces $\ell = n$ y $c = v_L(n) = n \cdot v_K(n)$, de modo que las condiciones (1') son válidas. Si $c \not\equiv 0 \pmod{n}$, entonces $c = -i + v_L(n-i) + v_L(a_{n-i})$ para algún i , $1 \leq i \leq n-1$, y $c < v_L(n) = n \cdot v_K(n)$. Pero, en este caso, $\ell = n-i$, y $v_L(a_{n-i}) - i > 0$; por tanto, $c > v_L(n-i) = v_L(\ell) = n \cdot v_K(\ell)$ y también se verifican las condiciones (1').

Recíprocamente, si $c \equiv 0 \pmod{n}$, entonces $\ell = n$ y $c = n \cdot v_K(n)$, de manera que cualquier polinomio $X^n - a_0$, con $a_0 \in p \setminus p^2$ genera una extensión L tal que $L \in \Sigma(n, n, c, K)$. En el caso en que $c \not\equiv 0 \pmod{n}$ observemos que, por (1'), el entero $c + n - \ell - n \cdot v_K(\ell)$ es un múltiplo no nulo de n ; de modo que existe por lo menos un $a_\ell \in A$ tal que $v_K(a_\ell) = n^{-1} \cdot (c + n - \ell - n \cdot v_K(\ell)) \geq 1$. Así, $a_\ell \in p$ y cualquier polinomio $f(X) = X^n + a_\ell X^\ell + a_0$, con $a_0 \in p \setminus p^2$, genera una extensión L tal que $L \in \Sigma(n, n, c, K)$.

COROLARIO. - En el caso equicaracterístico, y si $p \nmid e$, vemos que hay cuerpos con valor de Öre c para cada c no divisible por p ; en consecuencia, $\Sigma(n, e, K)$ es infinito.

NOTA. - En los demás casos, el conjunto de los valores de Öre es finito, y, por tanto, para demostrar la finitud de $\Sigma(n, e, K)$ basta con demostrar la finitud de $\Sigma(n, e, c, K)$ para todo valor de Öre c (cf. §3, fórmulas (5) y (6) y §4, fórmula (7)).

3. MASA DE UNA EXTENSIÓN LOCAL. FÓRMULAS DE SERRE. - Sea $L \in \Sigma(n, K)$. Consideremos la diferente

$$D(L|K) = p^{e-1+c(L|K)}$$

de la extensión $L|K$, y sea $f = f(P|p)$ el grado residual. El cuerpo residual $\bar{L}$ es finito con q^f elementos. Definimos la masa de la extensión $L|K$ como

$$\mu(L|K) = q^{-f \cdot c(L|K)},$$

es decir, $\mu(L|K)$ es el valor absoluto P -ádico (normalizado) de la componente *salvaje* de la diferente de la extensión.

Puesto que $c(L|K) = 0$ si y sólo si $p \nmid e$, se tiene que $\mu(L|K) = 1$ si y sólo si la extensión es moderadamente ramificada. Para el caso totalmente ramificado, es $f = 1$, y entonces $\mu(L|K) = q^{-c(L|K)}$ es la masa introducida por Serre en [4].

En este orden de ideas, Serre obtiene una interesante fórmula de ma-

sa que permite "contar" las extensiones separables totalmente ramificadas de un cuerpo local. Concretamente, Serre demuestra que

$$(3) \quad \sum_{L \in \Sigma(n, n, K)} \mu(L|K) = n.$$

En particular, para el caso moderadamente ramificado ($p \nmid n$) resulta que $\#\Sigma(n, n, K) = n$.

Teniendo en cuenta que las extensiones $L \in \Sigma(n, n, K)$ vienen definidas por polinomios de Eisenstein (2), y en virtud del lema de Krasner ([3], cap. II), Serre identifica el conjunto de tales polinomios con un subespacio abierto compacto de K^n . Considerando una base de B sobre A y medidas de Haar en L y en K, convenientemente normalizadas, calcula la medida del conjunto de los polinomios que definen un cuerpo fijo $L \in \Sigma(n, n, K)$ y la del conjunto de todos los polinomios separables de la forma (2). A través de la aplicación norma expresa el conjunto de los uniformizantes de B como un recubrimiento K-analítico étale del conjunto de los polinomios que definen L, de manera que consigue relacionar las medidas de estos dos conjuntos. Comparando éstas obtiene la fórmula (3).

Esta fórmula de masa de Serre admite la siguiente generalización:

PROPOSICIÓN. Con las notaciones anteriores se tiene que

$$(4) \quad \sum_{L \in \Sigma(n, e, K)} \mu(L|K) = e.$$

En particular, para el caso moderadamente ramificado, se obtiene que $\#\Sigma(n, e, K) = e$.

Demostración. Dado $L \in \Sigma(n, e, K)$, podemos considerar K_0 de manera que K_0 es no ramificado sobre K y L es totalmente ramificado sobre K_0 . Los grados respectivos son $[L:K_0] = e$ y $[K_0:K] = f = e^{-1} \cdot n$. Pero, extensiones $K_0|K$ no ramificadas, incluidas en K_S , y de grado f, sólo hay una (cf. [5], cap. III), de manera que se obtiene la igualdad

$$\Sigma(n, e, K) = \Sigma(e, e, K_0).$$

Por otra parte se tiene que $\mu(L|K_0) = q^{-f \cdot c(L|K_0)}$, puesto que $\#\bar{K}_0 = q^f = \#\bar{L}$ y $f(L|K_0) = 1$. Pero $c(L|K_0) = c(L|K)$, ya que $\mathcal{D}(L|K) = \mathcal{D}(L|K_0) \cdot \mathcal{D}(K_0|K)$, y $\mathcal{D}(K_0|K) = 1$. Luego $\mu(L|K_0) = \mu(L|K) = q^{-f \cdot c(L|K)}$.

En virtud de la fórmula de Serre (3) se tiene, por tanto, que

$$\sum_{L \in \Sigma(n, e, K)} \mu(L|K) = \sum_{L \in \Sigma(e, e, K_0)} \mu(L|K_0) = e,$$

como se trataba de demostrar.

Después de (3), Serre calcula la medida del conjunto de los polinomios de la forma (2) que definen un cuerpo fijo $L \in \Sigma(n, n, c, K)$, y utilizando los cálculos anteriores, obtiene que si c es un valor de Öre, entonces

$$(5) \quad \# \Sigma(n, n, c, K) = n \cdot \alpha(c) \cdot q^{-\beta(c)},$$

donde $\alpha(c)$ y $\beta(c)$ vienen dados por las expresiones

$$(6) \quad \alpha(c) = \begin{cases} 1 & \text{si } \ell = n \\ q^{-1} & \text{si } \ell \neq n \end{cases} \quad \text{y} \quad \beta(c) = \sum_{1 \leq i \leq n-1} \sup \left\{ 0, \left\lfloor \frac{c+i}{n} \right\rfloor - v_K(n-i) \right\}.$$

En particular, $\Sigma(n, n, c, K)$ siempre es finito.

4. FÓRMULAS DE KRASNER.- Por otra parte, Krasner obtiene también en [1] una fórmula para el cardinal de $\Sigma(n, n, c, K)$. Si c es un valor de Öre y ponemos

$$\rho = \left\lfloor \frac{c}{n \cdot v_K(p)} \right\rfloor \quad \text{y} \quad \gamma(c) = n \cdot v_K(p) \cdot (p^{-1} + \dots + p^{-\rho}) + \left\lfloor \frac{c - \rho \cdot n \cdot v_K(p)}{p^{\rho+1}} \right\rfloor,$$

entonces la fórmula de Krasner se puede escribir en la forma

$$(7) \quad \# \Sigma(n, n, c, K) = n \cdot \alpha(c) \cdot q^{\gamma(c)}.$$

Cuando K es un cuerpo p -ádico, el conjunto de los valores de Öre es finito; sumando las expresiones anteriores para todos los valores de c se obtiene que

$$(8) \quad \# \Sigma(n, n, K) = n \cdot \sum_{0 \leq s \leq v_p(n)} p^s \cdot (q^{\varepsilon(s) \cdot v_K(p)} - q^{\varepsilon(s-1) \cdot v_K(p)}),$$

donde $\varepsilon(0) = 0$, $\varepsilon(-1) = -\infty$, y $\varepsilon(s) = n \cdot (p^{-1} + \dots + p^{-s})$. A partir de esta fórmula, y descomponiendo cada extensión en una parte no ramificada y una totalmente ramificada, se obtiene la fórmula final

$$(9) \quad \# \Sigma(n, K) = \sum_{d|n} d \cdot \sum_{\substack{0 \leq s \\ p \nmid d, s \leq v_p(n)}} (p-1)^{-1} \cdot (p^{s+1+v_p(n)} - p^{2s}) \cdot (q^{\varepsilon(s) v_K(p)} - q^{\varepsilon(s-1) v_K(p)}).$$

Para demostrar (7), Krasner se basa en el lema que lleva su nombre (loc. cit.). A partir de una metrización conveniente del conjunto S_K de los polinomios unitarios e irreducibles de $K[X]$, y con el uso de subespacios adecuados de S_K , establece una relación entre el cardinal del conjunto $\Sigma(n, n, c, K)$ y el número de círculos de cierto radio contenidos en dichos subespacios. Después, debe calcular el número de estos círculos y compararlo con la relación antes obtenida.

5. EQUIVALENCIA DE LAS FÓRMULAS DE KRASNER Y DE SERRE.- Puesto que las condiciones de Öre no dependen de n , sino únicamente de e , las fórmulas de Serre (5) y de Krasner (7) pueden escribirse, respectivamente, en la forma

$$(10) \quad \# \Sigma(n, e, c, K) = e \cdot \alpha(e, c) \cdot q^f \cdot (c - \beta(e, c)),$$

$$(11) \quad \# \Sigma(n, e, c, K) = e \cdot \alpha(e, c) \cdot q^f \cdot \gamma(e, c);$$

donde $f = e^{-1} \cdot n$,

$$\alpha(e, c) = \begin{cases} 1 & \text{si } \ell = e \\ q^f - 1 & \text{si } \ell \neq e \end{cases}, \quad \beta(e, c) = \sum_{1 \leq i \leq e-1} \sup\{0, \left\lfloor \frac{c+i}{e} \right\rfloor - v_K(e-i)\},$$

$$\rho = \left\lfloor \frac{c}{e \cdot v_K(p)} \right\rfloor, \quad \gamma(e, c) = v_K(p) \cdot e \cdot (p^{-1} + \dots + p^{-\rho}) + \left\lfloor \frac{c - \rho \cdot e \cdot v_K(p)}{p^{\rho+1}} \right\rfloor,$$

y c satisface las condiciones (1) de Öre.

En efecto, descomponiendo $L|K$ en una extensión no ramificada y una totalmente ramificada, se tiene que $\Sigma(n, e, c, K) = \Sigma(e, e, c, K_0)$, $\bar{K}_0 = q^f$, $v_{K_0} = v_K$, y podemos aplicar entonces las fórmulas (5) y (7) para el caso $n=e$.

Es interesante demostrar la equivalencia de las fórmulas (10) y (11), puesto que ésto permite reobtener las fórmulas de Krasner (7), (8) y (9), a partir de la fórmula (5) de Serre.

NOTA: El mismo Krasner, en [2], demostró que su fórmula sobre $\# \Sigma(n, n, c, K)$ implica la fórmula de masas (3) de Serre.

Para ver la equivalencia de (10) y (11) probamos el siguiente:

TEOREMA.- Si c es un número natural que satisface las condiciones de Öre (1), entonces se tiene que

$$(12) \quad c = \gamma(e, c) + \beta(e, c).$$

Para la demostración de este teorema se utilizará el siguiente:

LEMA 1.- Sea $n = p^m \cdot h$ un número natural, con p primo, $m \geq 0$, y $(h, p) = 1$. Entonces, la valoración p -ádica de $n!$ viene dada por

$$v_p(n!) = n \cdot (p^{-1} + \dots + p^{-k}) + \sum_{1 \leq i \leq n} \sup\{0, (v_p(i) - k)\},$$

donde $0 \leq k \leq m$ es un natural arbitrario.

Demostración del lema.- El número de naturales i tales que $1 \leq i \leq n$, y con

$v_p(i) = j$ es exactamente $\left\lfloor \frac{n}{p^j} \right\rfloor - \left\lfloor \frac{n}{p^{j+1}} \right\rfloor$, para todo natural j .

Por tanto, $v_p(n!) = \sum_{j \geq 1} j \cdot ([n \cdot p^{-j}] - [n \cdot p^{-(j+1)}]) = \sum_{j \geq 1} [n \cdot p^{-j}]$.

Si $0 \leq k \leq m = v_p(n)$, podemos escribir $[n \cdot p^{-k}] = n \cdot p^{-k}$, y por tanto

$$v_p(n!) = n \cdot (p^{-1} + \dots + p^{-k}) + \sum_{j \geq k+1} [n \cdot p^{-j}].$$

De forma que el problema queda reducido a demostrar la igualdad

$$\sum_{j \geq k+1} [n \cdot p^{-j}] = \sum_{1 \leq i \leq n} \sup\{0, v_p(i) - k\},$$

para $0 \leq k \leq m$.

Pero $\sup\{0, v_p(i) - k\} = s > 0$ si y sólo si $v_p(i) = k + s$; es decir, si y sólo si $p^{k+s} | i$ y $p^{k+s+1} \nmid i$; el número de naturales i , $1 \leq i \leq n$, en estas condiciones es exactamente $[n \cdot p^{-(k+s)}] - [n \cdot p^{-(k+s+1)}]$, de manera que

$$\sum_{1 \leq i \leq n} \sup\{0, v_p(i) - k\} = \sum_{s \geq 1} s \cdot ([n \cdot p^{-(k+s)}] - [n \cdot p^{-(k+s+1)}]) = \sum_{s \geq 1} [n \cdot p^{-(k+s)}],$$

que es lo que se quería demostrar.

Demostración del teorema. - En virtud de las consideraciones anteriores, podemos limitarnos al caso totalmente ramificado ($e=n$), y basta con demostrar que si c es un natural que satisface las condiciones (1'), se tiene que

$$(13) \quad c = n \cdot v_K(p) \cdot (p^{-1} + \dots + p^{-\rho}) + \left\lfloor \frac{c - \rho \cdot n \cdot v_K(p)}{p^{\rho+1}} \right\rfloor + \sum_{1 \leq i \leq n-1} \sup\{0, \left\lfloor \frac{c+i}{n} \right\rfloor - v_K(n-i)\},$$

$$\text{con } \rho = \left\lfloor \frac{c}{n \cdot v_K(p)} \right\rfloor.$$

Hagamos la división entera de c por $n \cdot v_K(p)$, y pongamos

$$(14) \quad c = k \cdot n \cdot v_K(p) + j, \quad \text{con } 0 \leq j < n \cdot v_K(p) \text{ y } 0 \leq k \leq v_p(n).$$

$$\text{Entonces, } \rho = k \text{ y } \left\lfloor \frac{c - \rho \cdot n \cdot v_K(p)}{p^{\rho+1}} \right\rfloor = \left\lfloor \frac{j}{p^{k+1}} \right\rfloor.$$

De manera que para probar (13) basta probar que

$$(15) \quad k \cdot n \cdot v_K(p) + j = v_K(p) \cdot n \cdot (p^{-1} + \dots + p^{-k}) + [j \cdot p^{-(k+1)}] + \sum_{1 \leq i \leq n-1} \sup\{0, \left\lfloor \frac{j+i}{n} \right\rfloor + k \cdot v_K(p) - v_K(n-i)\}.$$

Teniendo en cuenta las condiciones de Öre (1'), se tiene que $j=0$, $j \equiv 0 \pmod{n}$, $\ell=n$, y $k=v_p(n)$ son propiedades equivalentes. Pero para $j=0$ se tiene que $\left\lfloor \frac{j}{p^{k+1}} \right\rfloor = 0$, $\left\lfloor \frac{j+i}{n} \right\rfloor = 0$ ($1 \leq i \leq n-1$), y puesto que $k=v_p(n)$ y $v_K(n) = v_p(n) \cdot v_K(p) = k \cdot v_K(p)$, se tiene que



$$\begin{aligned}
& v_K(p) \cdot n \cdot (p^{-1} + \dots + p^{-k}) + \sum_{1 \leq i \leq n-1} \sup\{0, k \cdot v_K(p) - v_K(n-i)\} - k \cdot n \cdot v_K(p) = \\
& = v_K(p) \cdot n \cdot (p^{-1} + \dots + p^{-k}) + \sum_{0 \leq i \leq n-1} \sup\{-k \cdot v_K(p), -v_K(n-i)\} = \\
& = v_K(p) \cdot n \cdot (p^{-1} + \dots + p^{-k}) + \sum_{0 \leq i \leq n-1} \sup\{0, v_K(n-i) - v_K(p) \cdot k\} - \sum_{0 \leq i \leq n-1} v_K(n-i) = \\
& = v_K(p) \cdot \left(n \cdot (p^{-1} + \dots + p^{-k}) + \sum_{0 \leq i \leq n-1} \sup\{0, v_p(n-i) - k\} \right) - v_K(p) \cdot v_p(n!) = 0,
\end{aligned}$$

la última igualdad en virtud del lema 1.

El problema queda, pues, reducido a demostrar (15) con las condiciones

$$(16) \quad c = k \cdot n \cdot v_K(p) + j, \quad 1 \leq j < n \cdot v_K(p), \quad j \not\equiv 0 \pmod{n}, \quad 0 \leq k < v_p(n).$$

Sumando $\sum_{1 \leq i \leq n-1} v_K(i) = \sum_{1 \leq i \leq n-1} v_K(n-i)$, y restando $(n-1) \cdot k \cdot v_K(p)$ a

los dos miembros de (15), hay que demostrar que

$$\begin{aligned}
(17) \quad k \cdot v_K(p) + \sum_{1 \leq i \leq n-1} v_K(i) + j &= v_K(p) \cdot n \cdot (p^{-1} + \dots + p^{-k}) + \left\lfloor \frac{j}{p^{k+1}} \right\rfloor + \\
&+ \sum_{1 \leq i \leq n-1} \sup\{v_K(n-i) - k \cdot v_K(p), \left\lfloor \frac{j+i}{n} \right\rfloor\}.
\end{aligned}$$

Puesto que $v_K(n) = \sup\{0, v_K(n) - k \cdot v_K(p)\} + k \cdot v_K(p)$, sumando a los dos lados $\sum_{1 \leq i \leq n-1} \sup\{0, v_K(n-i) - k \cdot v_K(p)\}$, y simplificando $v_p(n!)$, basta demostrar que

$$\begin{aligned}
(18) \quad \sum_{1 \leq i \leq n-1} \sup\{0, v_K(n-i) - k \cdot v_K(p)\} + j &= \left\lfloor \frac{j}{p^{k+1}} \right\rfloor + \\
&+ \sum_{1 \leq i \leq n-1} \sup\{v_K(n-i) - k \cdot v_K(p), \left\lfloor \frac{j+i}{n} \right\rfloor\}.
\end{aligned}$$

Pero $\frac{j+i}{n} < v_K(p) + \frac{1}{n}$, de manera que $\left\lfloor \frac{j+i}{n} \right\rfloor \leq v_K(p)$, $1 \leq i \leq n-1$. Para $v_p(n-i) > k$, resulta que $v_K(n-i) - k \cdot v_K(p) \geq v_K(p) \geq \left\lfloor \frac{j+i}{n} \right\rfloor$ y por lo tanto, los supremos correspondientes al sumando i en los dos miembros de la igualdad coinciden. Para $v_p(n-i) \leq k$, el supremo de la izquierda vale 0 y el de la derecha $\left\lfloor \frac{j+i}{n} \right\rfloor$. Simplificando, demostrar (18) equivale a demostrar que

$$(19) \quad j = \left\lfloor \frac{j}{p^{k+1}} \right\rfloor + \sum_{\substack{1 \leq i \leq n-1 \\ v_p(n-i) \leq k}} \left\lfloor \frac{j+i}{n} \right\rfloor,$$

para k, j , en las condiciones (16).

Hagamos ahora la división entera de j por n en la forma $j = \alpha n + \beta$. Las condiciones (16) para j y k equivalen a las condiciones, para α, β ,

$$(20) \quad j = \alpha n + \beta, \quad 1 \leq \beta < n, \quad 0 \leq \alpha < v_p(p),$$

y substituyendo j en (19), el problema queda reducido a demostrar que

$$(21) \quad \alpha n + \beta = \alpha n \cdot p^{-(k+1)} + [\beta \cdot p^{-(k+1)}] + \sum_{\substack{1 \leq i \leq n-1 \\ v_p(n-i) \leq k}} (\alpha + \left\lfloor \frac{\beta+i}{n} \right\rfloor), \quad k < v_p(n).$$

Pero $v_p(n-i) \leq k$ equivale a $v_p(i) \leq k$, puesto que $k < v_p(n)$. Entonces, el número de sumandos α que aparecen en el segundo miembro coincide con el número de naturales i , $1 \leq i \leq n-1$, no divisibles por p^{k+1} ; puesto que n es divisible por p^{k+1} , este número vale $n - \{n/p^{k+1}\} = n - \alpha \cdot p^{-(k+1)}$. Simplificando, (21) equivale a demostrar que

$$(22) \quad \beta = [\beta \cdot p^{-(k+1)}] + \sum_{\substack{1 \leq i \leq n-1 \\ v_p(n-i) \leq k}} \left\lfloor \frac{\beta+i}{n} \right\rfloor,$$

para $k < v_p(n)$ y β en las condiciones (20).

Pero

$$\left\lfloor \frac{\beta+i}{n} \right\rfloor = \begin{cases} 0 & \text{si } 1 \leq i < n - \beta \\ 1 & \text{si } 1 \leq n - i \leq \beta \quad (n - \beta \leq i \leq n - 1). \end{cases}$$

Por tanto, el sumatorio de (22) coincide con el número de naturales $n-i$, con $1 \leq n-i \leq \beta$, y $n-i$ no divisible por p^{k+1} ; es decir, es exactamente

$$\beta - \left\lfloor \frac{\beta}{p^{k+1}} \right\rfloor,$$

con lo cual queda demostrada la fórmula (22) y, en consecuencia, la (12).

COROLARIO.— Las fórmulas (10) y (11) son equivalentes. En particular (11) se obtiene a partir de (10).

BIBLIOGRAFÍA, —

- 1 M.KRASNER: *Nombre des extensions d'un degré donné d'un corps P-adique.* Colloques Internationaux du C.N.R.S. 143 (1966), pp. 143-169.
- 2 M.KRASNER: *Remarques au sujet d'une note de J.-P.Serre:.....* C.R.Acad.Sc.Paris. 288 (1979), série A, pp. 863-865.
- 3 S.LANG: *Algebraic number theory.* Addison Wesley, 1970.
- 4 J.-P.SERRE: *Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local.* C.R.Acad.Sc.Paris. 286 (1978), série A, pp. 1031-1036.

[5] J.P.SERRE: *Local fields*. GTM 67. Springer-Verlag (1979) (Primera ed. 1968).

Artur Travesa Grau

Departament d'Àlgebra i Fonaments

Facultat de Matemàtiques

Universitat de Barcelona

Gran via de les Corts Catalanes, 585

Barcelona 08007. ESPANYA.

Presentado como ponencia en las "X Jornadas Hispano-Lusas de Matemáticas".



publicacions
edicions
universitat
de barcelona



Dipòsit Legal, B.: 9.902-1986
BARCELONA-1986