UNIVERSITAT DE BARCELONA

Extensiones maximales de un cuerpo global en las que un divisor primo descompone completamente

Pilar Báyer Isant

UNIVERSIDAD DE BARCELONA

FACULTAD DE MATEMATICAS

EXTENSIONES MAXIMALES DE UN CUERPO GLOBAL EN LAS QUE UN DIVISOR PRIMO DESCOMPONE COMPLETAMENTE

Memoria presentada por
Pilar Báyer Isant
para optar al grado de
Doctor en Ciencias,
Sección de Matemáticas.

Barcelona , 1974 .

Contenido

INTRODUCCION

Dado un cuerpo global K y un conjunto finito $\mathfrak{p}_1,\dots,\mathfrak{p}_r$ de primos de K, representamos por $K_{\mathfrak{p}_1,\dots,\mathfrak{p}_r}$ la extensión maximal de K contenida en una clausura separable $\overline{K}$ de K, en la que todos los primos $\mathfrak{p}_i$ descomponen completamente. Esta memoria tiene por objeto el estudio de tales extensiones.

Los cuerpos $K_{\mathfrak{p}_1,\dots,\mathfrak{p}_r}$ se identifican con subcuerpos del completado de K en $\mathfrak{p}_i$, $\hat{K}_{\mathfrak{p}_i}$, para $i = 1,\dots,r$ y se pueden obtener a partir de los cuerpos fijos de los normalizados de los grupos de descomposición, cuya importancia ha sido destacada en [45].

La denominación que se propone para $K_{\mathfrak{p}_1,\dots,\mathfrak{p}_r}$ es la de cuerpo totalmente $\mathfrak{p}$-ádico (relativo a los primos $\mathfrak{p}_1,\dots,\mathfrak{p}_r$), debido a que generalizan el concepto de cuerpo totalmente real clásico.

Si L es una extensión finita y galoisiana de K, $\mathfrak{p}$ un primo de K y $\mathfrak{p}_i$, $1 \leq i \leq g$, son los divisores primos de $\mathfrak{p}$ en L, $L_{\mathfrak{p}_1,\dots,\mathfrak{p}_g}$ es siempre una extensión de Galois de $K_{\mathfrak{p}}$, mientras que el carácter galoisiano de $L_{\mathfrak{p}}/K_{\mathfrak{p}}$ permite caracterizar aquellas extensiones L/K cuyo grupo de descomposición $D_{\mathfrak{p}}(L/K)$ es normal en el grupo de Galois $G(L/K)$.

La extensión abeliana maximal de K contenida en $K_{\mathfrak{p}_1,\dots,\mathfrak{p}_r}$ es de grado no finito sobre K. La ley de

reciprocidad de Artin permite dar una condición necesaria y suficiente sobre los primos $\mathfrak{p}_i$ a fin de que, cuando K es un cuerpo de números, el " Hilbert Class Field " de K esté contenido en $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$.

Antes de emprender el estudio de ecuaciones diofánticas sobre los cuerpos $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ se analiza su grupo de Brauer. Se obtiene que $B(K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r})$ contiene un subgrupo isomorfo al producto cartesiano de los grupos de Brauer $B(\hat{K}_{\mathfrak{p}_1}) \times \ldots \times B(\hat{K}_{\mathfrak{p}_r})$. Una de las consecuencias que de este resultado se derivan, es la existencia de extensiones normales, para cualquier cuerpo de números K , que presentan en un conjunto finito de primos de K normalizados no resolubles de los grupos de descomposición.

La finitud del índice $(K^* K_{\mathfrak{p}}^{*n} : K_{\mathfrak{p}}^{*n})$, para ciertos valores de n , es aplicada a la discusión de formas diagonales definidas en el cuerpo K . Contrariamente a lo que ocurre en el caso $\mathfrak{p}$-ádico, el índice $(K_{\mathfrak{p}}^* : K_{\mathfrak{p}}^{*n})$ se demuestra que, en general, es infinito.

Finalmente, a través de las extensiones $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ se presenta una nueva formulación del principio de Hasse que, sin destruir las situaciones de validez clásicas, incorpora otras en las que no se verifica el principio de Hasse tradicional.

Deseo expresar mi agradecimiento en primer lugar al Dr. R. Mallol, director del trabajo. Al Dr. F. Tomás por haberme dado a conocer sus artículos [45] y [46] y por

sus sugerencias. Al Dr. E. Linés cuyos cursos despertaron mi interés por la Teoría de Números y a Dña. Griselda Pascual por su constante estímulo y ayuda.

Capítulo I

CUERPOS TOTALMENTE $\mathfrak{p}$-ADICOS

Introducción.

Sea K un cuerpo y $\mathfrak{p}$ una clase de valoraciones discretas de K, o bien una clase de valores absolutos no ultramétricos, en el sentido de Bourbaki [5].

En este capítulo se introducen los cuerpos $K_{\mathfrak{p}}$ como las extensiones maximales de K, contenidas en una clausura separable $\overline{K}$, en las que $\mathfrak{p}$ descompone completamente.

Los cuerpos $K_{\mathfrak{p}}$ se caracterizan como subcuerpos del completado de K en $\mathfrak{p}$, $\hat{K}_{\mathfrak{p}}$. Si $\hat{K}_{\mathfrak{p}}$ es isomorfo al cuerpo real y K se considera incluido en R, $K_{\mathfrak{p}}$ coincide con la unión de todas las extensiones de grado finito y totalmente reales sobre K, es decir, cuya clusura galoisiana sobre K está contenida en R. En el caso discreto se obtiene para $K_{\mathfrak{p}}$ una caracterización análoga en términos de $\hat{K}_{\mathfrak{p}}$. De ahí que para designar a tales cuerpos se haya elegido la denominación de <u>cuerpos totalmente $\mathfrak{p}$-ádicos</u>.

De la definición de $K_{\mathfrak{p}}$ resulta que $K_{\mathfrak{p}}/K$ es una extensión galoisiana; su grupo de Galois, así como el de $\overline{K}/K_{\mathfrak{p}}$, es calculado en función de los normalizados de los grupos de descomposición de los divisores primos de $\mathfrak{p}$ en las extensiones de K, de grado finito y normales, contenidas en $\overline{K}$.

1. Notaciones y propiedades generales

En este apartado y en el siguiente se indicará por A a un anillo de Dedekind y por K a su cuerpo de fracciones.

Si L es una extensión de K de grado finito, la clausura entera B de A en L es un anillo de Dedekind ([6], § 2, nº 5, Cor. 3 de la Prop. 5). Sea $\mathfrak{P}$ un ideal primo no nulo de B y $\mathfrak{p} = \mathfrak{P} \cap A$; el exponente $e_{\mathfrak{P}}$ de $\mathfrak{P}$ en la descomposición de $\mathfrak{p}B$ en ideales primos de B,

$$\mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}}$$

y el grado $f_{\mathfrak{P}}$ de la extensión $B/\mathfrak{P}$ de $A/\mathfrak{p}$ se denominan el índice de ramificación y el grado residual de $\mathfrak{P}$, respectivamente, en la extensión L/K.

Si $n = [L : K]$, se verifica la relación

$$\sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}} \leq n \quad ,$$

siendo válido el signo de igualdad cuando L es una extensión separable de K.

Dado un ideal primo $\mathfrak{p}$ de A, la topología asociada a la valoración $\mathfrak{p}$-ádica de K, $v_{\mathfrak{p}}$, convierte a K en un cuerpo topológico. Se indicará por $\hat{K}_{\mathfrak{p}}$ al correspondiente completado. $\hat{K}_{\mathfrak{p}}$ es a su vez un cuerpo valorado cuya valoración extiende la de K.

Si a es un número real tal que $0 < a < 1$, la fórmula

$$\| x \| = a^{v_{\mathfrak{p}}(x)} \quad , \quad x \in K \quad ,$$

define en K un valor absoluto ultramétrico ; la topología de K asociada al mismo no depende del número a elegido y coincide con la obtenida a través de $v_{\mathfrak{p}}$.

La completación de L en $\mathfrak{P}$, $\hat{L}_{\mathfrak{P}}$, - notación anterior - , proporciona una extensión finita de $\hat{K}_{\mathfrak{p}}$. El grado

$$n_{\mathfrak{P}} = \left[\hat{L}_{\mathfrak{P}} : \hat{K}_{\mathfrak{p}} \right]$$

se denomina el grado local de $\mathfrak{P}$ en la extensión L/K y se verifica

$$n_{\mathfrak{P}} = e_{\mathfrak{P}} f_{\mathfrak{P}} \ .$$

Si la extensión L/K es de Galois , su grupo de Galois G opera transitivamente en el conjunto de los ideales primos de B que dividen a un ideal primo $\mathfrak{p}$ de A dado . Si $\mathfrak{P}$ es uno de estos divisores , por $D_{\mathfrak{P}}(L/K)$ se indica en grupo de descomposición de $\mathfrak{P}$ en la extensión L/K ; es decir ,

$$D_{\mathfrak{P}}(L/K) = \left\{ \sigma \in G \ ; \ \sigma(\mathfrak{P}) = \mathfrak{P} \right\} .$$

Si $\mathfrak{P}$ es un ideal primo no nulo de B , el orden de $D_{\mathfrak{P}}(L/K)$ es igual al grado local $n_{\mathfrak{P}}$.

Los grupos de descomposición $D_{\mathfrak{P}}(L/K)$, $D_{\mathfrak{P}'}(L/K)$, correspondientes a dos divisores primos $\mathfrak{P}$ y $\mathfrak{P}'$ de un mismo ideal primo $\mathfrak{p}$ de A , son conjugados en G .

2. Introducción de los cuerpos $K_{\mathfrak{p}}$

Definición (2.1).- Un ideal primo $\mathfrak{p}$ de A se dice que descompone completamente en una extensión L de K de grado finito n , si existen en la clausura entera B

de A en L, n ideales primos distintos que dividen a $\mathfrak{p}$.

Cuando L es una extensión separable de K, la condición anterior es equivalente a que

$$L \underset{K}{\otimes} \hat{K}_{\mathfrak{p}} \simeq \hat{K}_{\mathfrak{p}} \times \overset{(n}{\ldots} \times \hat{K}_{\mathfrak{p}} .$$

El conjunto de los ideales primos de A que descomponen completamente en L se indicará por $S(B/A)$ o por $S(L/K)$, siempre que no haya lugar a confusión.

Si M es una extensión algebraica de K de grado no finito, diremos que $\mathfrak{p}$ descompone completamente en M cuando

$$\mathfrak{p} \in S(L/K)$$

para toda subextensión L de M, de grado finito sobre K.

En lo sucesivo, todas las extensiones algebraicas de K se considerarán incluidas en una misma clausura algebraica $\overline{K}$ de K.

<u>Proposición (2.2).-</u> Sean L_1 y L_2 dos extensiones finitas y separables de K y sea L la composición L_1L_2. Si por A_i indicamos la clausura entera de A en L_i y por B la de A en L, se verifica

$$S(A_1/A) \cap S(A_2/A) = S(B/A) .$$

Demostración :

Sea $\mathfrak{P}$ un ideal primo no nulo de B, $\mathfrak{P}_i = \mathfrak{P} \cap A_i$ y $\mathfrak{p} = \mathfrak{P} \cap A$. Las relaciones

$$e_{\mathfrak{P}}(L/K) = e_{\mathfrak{P}}(L/L_i)\, e_{\mathfrak{P}_i}(L_i/K)$$

$$f_{\mathfrak{P}}(L/K) = f_{\mathfrak{P}}(L/L_i)\, f_{\mathfrak{P}_i}(L_i/K)$$

ponen de manifiesto la inclusión

$$S(B/A) \subset S(A_1/A) \cap S(A_2/A) \ .$$

Para probar la inclusión en el sentido contrario pasaremos a los completados de K y de L en $\mathfrak{p}$ y en $\mathfrak{P}$, respectivamente. Es sabido ([39], Cap. 2, § 3, Cor. 1 al Teor. 1) que existe un K-monomorfismo σ de L en una clausura algebraica de $\hat{K}_{\mathfrak{p}}$, de modo que $\hat{L}_{\mathfrak{P}} = \hat{K}_{\mathfrak{p}}(\sigma L)$. La restricción σ_i de σ a L_i permite a su vez obtener los completados de L_i en $\mathfrak{P}_i$. Si

$$\mathfrak{p} \in S(A_1/A) \cap S(A_2/A) \ ,$$

se tendrá en consecuencia

$$\hat{K}_{\mathfrak{p}} = \hat{K}_{\mathfrak{p}}(\sigma_i L_i) \quad , \quad \text{para} \quad i = 1, 2 \ ,$$

y, ya que $\sigma L = (\sigma_1 L_1)(\sigma_2 L_2)$, $\hat{L}_{\mathfrak{P}} = \hat{K}_{\mathfrak{p}}$. Al recorrer $\mathfrak{P}$ todos los divisores primos de $\mathfrak{p}$ en B se obtendrá que $\mathfrak{p} \in S(B/A)$.

Definición (2.3).- Denominamos cuerpo totalmente $\mathfrak{p}$-ádico relativo a un ideal primo $\mathfrak{p}$ de A a la reunión filtrante de las extensiones finitas y separables de K en las que $\mathfrak{p}$ descompone completamente. Dicho cuerpo lo representaremos por $K_{\mathfrak{p}}$.

De manera equivalente, puede definirse $K_{\mathfrak{p}}$ como la

máxima extensión separable de K en la que $\mathfrak{p}$ descompone completamente.

Puesto que el grado residual y el índice de ramificación se conservan por localización , $K_{\mathfrak{p}}$ depende únicamente del anillo de la valoración de K asociada a $\mathfrak{p}$.

Si $\mathfrak{p}$ es el ideal nulo , de la definición resulta que $K_{\mathfrak{p}} = K$, por lo que este caso no será tenido en cuenta en general.

Definición (2.3').- Si A_i , $i=1,\dots,r$, es una familia finita de anillos de valoración discreta , de ideales maximales $\mathfrak{p}_i$ y de cuerpo de fracciones K , por cuerpo totalmente $\mathfrak{p}$-ádico relativo a los ideales $\mathfrak{p}_1,\dots,\mathfrak{p}_r$, entenderemos la máxima extensión separable de K en la que todos los ideales $\mathfrak{p}_i$ descomponen completamente . Será representado por $K_{\mathfrak{p}_1,\dots,\mathfrak{p}_r}$. Se tendrá

$$K_{\mathfrak{p}_1,\dots,\mathfrak{p}_r} = \bigcap_{i=1}^{r} K_{\mathfrak{p}_i} .$$

Proposición (2.4).- Un elemento $x \in \overline{K}$, separable sobre K , es de $K_{\mathfrak{p}}$ si y sólo si su polinomio minimal sobre K descompone en factores lineales en $\hat{K}_{\mathfrak{p}}$.

Demostración :

Sea $L = K(x)$. Por ser x un elemento primitivo de L/K , el polinomio minimal de x sobre K coincidirá con el polinomio característico de x en la citada extensión ([5o], Cap.II, § 1o, Teor. 2o). Sea B la clausura entera

de A en L y para cada divisor primo $\mathfrak{P}_i$ de $\mathfrak{p}$ en B, sea σ_i un K-monomorfismo de L en una clausura algebraica de $\hat{K}_\mathfrak{p}$, de modo que $\hat{L}_{\mathfrak{P}_i} = \hat{K}_\mathfrak{p}(\sigma_i L)$. El polinomio característico de x en la extensión L/K es igual al producto de los polinomios característicos de los elementos $\sigma_i(x)$ en las extensiones $\hat{L}_{\mathfrak{P}_i}/\hat{K}_\mathfrak{p}$ ([39], Cap.II, § 3, Cor. 2 al Teor. 1). La demostración concluye al tener en cuenta que $\sigma_i(x)$ es un elemento primitivo de $\hat{L}_{\mathfrak{P}_i}$ sobre $\hat{K}_\mathfrak{p}$.

3. Consideración del caso no ultramétrico

Se introducen en este apartado los cuerpos $K_\mathfrak{p}$ relativos a los valores absolutos no ultramétricos de K. Es decir, se construyen los cuerpos $K_\mathfrak{p}$, cuando $\mathfrak{p}$ es un "primo infinito" de K.

Según el teorema de Ostrowski ([5],Cap.VI,§6, nº4,Teor.2), un cuerpo K dotado de un valor absoluto no ultramétrico es necesariamente isomorfo a un subcuerpo del cuerpo complejo $\mathbb{C}$; existe un único número real s, $0 < s \leq 1$, y existe un monomorfismo $\sigma : K \longrightarrow \mathbb{C}$, de modo que el valor absoluto de K viene dado por

$$\| x \| = |\sigma(x)|^s \quad .$$

En todo este apartado se supondrá que K es isomorfo a un subcuerpo de $\mathbb{C}$.

Definición (3.1).- Denominaremos primos infinitos de K a las clases de valores absolutos no ultramétricos

de K (llamando equivalentes a aquellos valores absolutos que sobre K definen la misma topología). Se indicarán con la notación $\mathfrak{p}_\infty$.

La completación de K en $\mathfrak{p}_\infty$, $\hat{K}_{\mathfrak{p}_\infty}$, es un cuerpo isomorfo a R o a $\mathbb{C}$. En el primer caso se dirá que $\mathfrak{p}_\infty$ es un <u>primo real</u> y en el segundo , un <u>primo complejo</u> .

Si L es una extensión algebraica de K y $\mathfrak{P}_\infty$ es un primo infinito de L cuya restricción a K es $\mathfrak{p}_\infty$, diremos que $\mathfrak{P}_\infty$ divide a $\mathfrak{p}_\infty$. El grado correspondiente

$$n_{\mathfrak{P}_\infty} = \left[\hat{L}_{\mathfrak{P}_\infty} : \hat{K}_{\mathfrak{p}_\infty} \right]$$

se denomina el grado local de $\mathfrak{P}_\infty$ en la extensión L/K . Obviamente $n_{\mathfrak{P}_\infty} = 1$, ó $n_{\mathfrak{P}_\infty} = 2$.

Si $n = \left[L : K \right]$ se verifica la relación

$$n = \sum_{\mathfrak{P}_\infty \mid \mathfrak{p}_\infty} n_{\mathfrak{P}_\infty} .$$

En el caso en que $\mathfrak{p}_\infty$ sea un primo real , la relación anterior se traduce en

$$n = r_1 + 2r_2$$

en donde r_1 es el número de primos reales de L y r_2 es el número de primos complejos que dividen a $\mathfrak{p}_\infty$.

<u>Definición (3.2).-</u> Un primo $\mathfrak{p}_\infty$ de K se dice que <u>descompone completamente</u> en una extensión finita L de K de grado n cuando existen en L n primos distintos

que dividen a $\mathfrak{p}_\infty$.

De forma equivalente , $\mathfrak{p}_\infty$ descompone completamente en L si se verifica

$$L \underset{K}{\otimes} \hat{K}_{\mathfrak{p}_\infty} \simeq \hat{K}_{\mathfrak{p}_\infty} \times \overset{(n}{\ldots} \times \hat{K}_{\mathfrak{p}_\infty} .$$

De la definición resulta que si $\mathfrak{p}_\infty$ es un primo complejo, siempre descompone completamente . Si $\mathfrak{p}_\infty$ es un primo real , descompone completamente en L si y sólo si $r_2 = o$.

Definición (3.3).- Dado un primo infinito de K , $\mathfrak{p}_\infty$, representaremos por $K_{\mathfrak{p}_\infty}$ a la reunión filtrante de las extensiones finitas de K en las que $\mathfrak{p}_\infty$ descompone completamente.

Si $\mathfrak{p}_\infty$ es un primo complejo , $K_{\mathfrak{p}_\infty}$ será igual a la clausura algebraica $\bar{K}$ de K . Si $\mathfrak{p}_\infty$ es real , denominaremos a $K_{\mathfrak{p}_\infty}$ el cuerpo totalmente real asociado a K y a $\mathfrak{p}_\infty$.

Proposición (3.4).- Un elemento $x \in \bar{K}$ es de $K_{\mathfrak{p}_\infty}$ si y sólo si su polinomio minimal sobre K descompone en factores lineales en $\hat{K}_{\mathfrak{p}_\infty}$.

Demostración :

Si $\mathfrak{p}_\infty$ es un primo complejo , la proposición es trivial.

Supongamos que $\mathfrak{p}_\infty$ es un primo real . Sea $L = K(x)$ y sean $\mathfrak{P}_{\infty,i}$ $(i = 1,\ldots,r_1 + r_2)$, los divisores de $\mathfrak{p}_\infty$ en

L . Sea $\| \ \| \in \mathfrak{p}_\infty$ y $\sigma : K \longrightarrow \mathbb{C}$ un monomorfismo tal que

$$\| y \| = |\sigma(y)|^s \quad , \text{ para } \quad y \in K \ .$$

Para cada i , existirá una extensión $\sigma_i : L \longrightarrow \mathbb{C}$ de σ , de modo que

$$\hat{L}_{\mathfrak{P}_{\infty,i}} \simeq R(\sigma_i(L)) = R(\sigma_i(x)) \ .$$

En consecuencia, $\hat{L}_{\mathfrak{P}_{\infty,i}}$ será isomorfo a R para todo i si y sólo si , para todo i , $\sigma_i(x) \in R$. Ello es equivalente a que la imagen por σ del polinomio minimal de x sobre K tenga todas sus raíces reales.

Observación (3.5).- Si $K = Q$ la clase del valor absoluto es el único primo infinito ; el correspondiente cuerpo asociado , Q_∞ , es la unión de todas las extensiones finitas de Q totalmente reales en el sentido clásico, es decir es la unión de las extensiones $Q(x)$ de Q cuyos conjugados son todos reales . Ello justifica la denominación dada en el apartado 2 a los cuerpos $K_\mathfrak{p}$.

4. El grupo de Galois $G(\overline{K}/K_\mathfrak{p})$

En este apartado K indicará un cuerpo y $\overline{K}$ una clausura separable del mismo . Todas las extensiones algebraicas de K que se consideran se suponen incluidas en $\overline{K}$.

Proposición (4.1).- Sea A un anillo de Dedekind , K su cuerpo de fracciones y $\mathfrak{p}$ un ideal primo de A .

Sea L una extensión finita y galoisiana de K de grupo de Galois $G(L/K)$ y sea B la clausura entera de A en L. Indiquemos por $N_{\mathfrak{p}}(L/K)$ el subgrupo normal de $G(L/K)$ generado por uno cualquiera de los grupos de descomposición $D_{\mathfrak{P}}(L/K)$, de un divisor primo $\mathfrak{P}$ de $\mathfrak{p}$ en B.

Si $K_{\mathfrak{p}}$ es el cuerpo totalmente $\mathfrak{p}$-ádico relativo a $\mathfrak{p}$, el grupo de Galois de la extensión $L/L\cap K_{\mathfrak{p}}$ viene dado por

$$G(L/L\cap K_{\mathfrak{p}}) = N_{\mathfrak{p}}(L/K) \ .$$

Demostración :

De la definición de $K_{\mathfrak{p}}$ se sigue que $L\cap K_{\mathfrak{p}}$ es la máxima subextensión de L en la que $\mathfrak{p}$ descompone completamente. Sea $L^{D_{\mathfrak{P}}}$ el subcuerpo de L fijo por $D_{\mathfrak{P}}(L/K)$, $\overline{B}$ la clausura entera de A en $L^{D_{\mathfrak{P}}}$ y $\overline{\mathfrak{P}} = \mathfrak{P}\cap\overline{B}$. Es sabido que ([39], Cap.I, § 7, Prop.21) :

$$e_{\overline{\mathfrak{P}}}(L/L^{D_{\mathfrak{P}}}) = e_{\mathfrak{p}}(L/K)$$

$$f_{\overline{\mathfrak{P}}}(L/L^{D_{\mathfrak{P}}}) = f_{\mathfrak{p}}(L/K) \ ,$$

lo cual implica

$$e_{\overline{\mathfrak{P}}}(L^{D_{\mathfrak{P}}}/K) = f_{\overline{\mathfrak{P}}}(L^{D_{\mathfrak{P}}}/K) = 1 \ .$$

Ya que el subcuerpo de L fijo por $N_{\mathfrak{p}}(L/K)$ vendrá dado por

$$L^{N_{\mathfrak{p}}} = \bigcap_{\mathfrak{P}|\mathfrak{p}} L^{D_{\mathfrak{P}}} \ ,$$

se obtiene que $\mathfrak{p} \in S(L^{N_{\mathfrak{p}}}/K)$ y, por tanto,

$$L^{N_{\mathfrak{p}}} \subset L\cap K_{\mathfrak{p}} \ .$$

Sea C la clausura entera de A en $L \cap K_\mathfrak{p}$ y $\mathfrak{p}' = \mathfrak{p} \cap C$. Puesto que $K_\mathfrak{p}/K$ es una extensión de Galois (basta tener en cuenta (2.4)), la extensión $L \cap K_\mathfrak{p}/K$ será de Galois. Por restricción se obtendrá un epimorfismo de

$$D_\mathfrak{p}(L/K) \longrightarrow D_{\mathfrak{p}'}(L \cap K_\mathfrak{p}/K) .$$

Puesto que $D_{\mathfrak{p}'}(L \cap K_\mathfrak{p}/K) = (1)$, se obtiene la inclusión

$$L \cap K_\mathfrak{p} \subset L^{D_\mathfrak{p}}$$

y por tanto, la de $L \cap K_\mathfrak{p} \subset L^{N_\mathfrak{p}}$. Ello concluye la demostración, habida cuenta de que L/K es una extensión finita.

Teorema (4.2).- Sea A un anillo de Dedekind , K su cuerpo de fracciones y $\mathfrak{p}$ un ideal primo de A . Sea M una extensión finita y de Galois de K y L una extensión galoisiana de K contenida en M .

La proyección canónica de $G(M/K)$ en $G(L/K)$ aplica $N_\mathfrak{p}(M/K)$ exhaustivamente en $N_\mathfrak{p}(L/K)$. El conjunto de los grupos $N_\mathfrak{p}(L/K)$ obtenidos al recorrer L las extensiones finitas y galoisianas de K , juntamente con las proyecciones mencionadas, constituye un sistema proyectivo de grupos, verificándose

$$G(\overline{K}/K_\mathfrak{p}) = \varprojlim_L N_\mathfrak{p}(L/K) . .$$

Demostración :

La primera de las afirmaciones resulta de la definición

de los $N_{\mathfrak{p}}$ (4.1) , y de ser válida dicha propiedad a nivel de grupos de descomposición.

Un simple cálculo prueba que la familia de las extensiones $LK_{\mathfrak{p}}$ de $K_{\mathfrak{p}}$ obtenida al recorrer L el conjunto de las extensiones finitas y de Galois de K contenidas en $\overline{K}$ es cofinal en el conjunto de las extensiones de Galois y finitas de $K_{\mathfrak{p}}$. En consecuencia , al recorrer L el citado conjunto se obtendrá

$$G(\overline{K}/K_{\mathfrak{p}}) = G(\varinjlim_{L} LK_{\mathfrak{p}}/K_{\mathfrak{p}}) = \varprojlim_{L} G(LK_{\mathfrak{p}}/K_{\mathfrak{p}})$$

- para la última igualdad, véase por ejemplo [32], exp. 3 - . Puesto que

$$G(LK_{\mathfrak{p}}/K_{\mathfrak{p}}) \simeq G(L/L\cap K_{\mathfrak{p}}) ,$$

la demostración concluye a partir del resultado obtenido en (4.1) .

Corolario (4.3).- Al recorrer L el conjunto de las extensiones finitas y de Galois de K , para el grupo de Galois $G(K_{\mathfrak{p}}/K)$ se obtiene la siguiente expresión

$$G(K_{\mathfrak{p}}/K) = \varprojlim_{L} \frac{G(L/K)}{N_{\mathfrak{p}}(L/K)} .$$

Observación (4.4).- La teoría de los grupos de ramificación puede llevarse a cabo en extensiones no finitas. Considerando los grupos de descomposición $D_{\mathfrak{P}}(\overline{K}/K)$ para cada "divisor primo" $\mathfrak{P}$ de $\mathfrak{p}$ en $\overline{K}$, así como los

subgrupos normales $N_p(\overline{K}/K)$ que éstos generan en $G(\overline{K}/K)$, el grupo de Galois de $\overline{K}/K_p$ coincide con la adherencia de $N_p(\overline{K}/K)$ en $G(\overline{K}/K)$, al dotar a este último grupo de la topología de Krull ; a tal fin, véase [45] .

Capítulo II

EXTENSIONES

Introducción.

Sea A un anillo de valoración discreta, de ideal maximal $\mathfrak{p}$ y de cuerpo de fracciones K. Dada una extensión finita y de Galois L de K, si B es la clausura entera de A en L y $\mathfrak{P}$ un divisor primo de $\mathfrak{p}$ en B, es sabido que el grupo de descomposición $D_{\mathfrak{P}}(L/K)$, en general no es un subgrupo normal de $G(L/K)$. Al considerar los cuerpos $L_{\mathfrak{P}}$ y $K_{\mathfrak{p}}$ se obtiene que $L_{\mathfrak{P}}$ es una extensión de $K_{\mathfrak{p}}$ no necesariamente galoisiana (a diferencia de lo que ocurre en el caso $\mathfrak{p}$-ádico con las extensiones $\hat{L}_{\mathfrak{P}}/\hat{K}_{\mathfrak{p}}$). El hecho de que $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ sea galoisiana permite caracterizar aquellas extensiones L de K en las que $D_{\mathfrak{P}}(L/K)$ es un subgrupo normal de $G(L/K)$.

Si a partir de L y de K se desean obtener, mediante cuerpos totalmente $\mathfrak{p}$-ádicos, extensiones galoisianas, deben tenerse en cuenta todos los divisores primos $\mathfrak{P}_1,\dots,\mathfrak{P}_g$ de $\mathfrak{p}$ en B. Si L/K es de Galois, la extensión $L_{\mathfrak{P}_1,\dots,\mathfrak{P}_g}/K_{\mathfrak{p}}$ es siempre galoisiana.

En el caso de ser K un cuerpo global, para toda elección finita de primos de K, la extensión abeliana maximal de K contenida en $K_{\mathfrak{p}_1,\dots,\mathfrak{p}_r}$ resulta ser una extensión de K no finita.

En el último apartado, se comparan los cuerpos $K_{\mathfrak{p}}$

obtenidos a partir de un cuerpo de números K con el "Hilbert Class Field", K_1, del mismo. La ley de reciprocidad de Artin permite obtener una condición necesaria y suficiente sobre $\mathfrak{p}$ a fin de que K_1 sea un subcuerpo de $K_{\mathfrak{p}}$.

1. Las extensiones $L_{\mathfrak{P}}$ de $K_{\mathfrak{p}}$

Todas las extensiones algebraicas del cuerpo K se considerarán incluidas en una misma clausura algebraica $\overline{K}$.

Teorema (1.1).- Sea A un anillo de valoración discreta, $\mathfrak{p}$ su ideal maximal y K su cuerpo de fracciones. Sea L una extensión finita y de Galois de K, B la clausura entera de A en L y $\mathfrak{P}$ un divisor primo de $\mathfrak{p}$ en B. Las siguientes afirmaciones son entonces equivalentes :

a) $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ es una extensión galoisiana.

b) La restricción a L de todo $K_{\mathfrak{p}}$-monomorfismo de $L_{\mathfrak{P}}$ en $\overline{K}$ pertenece al grupo de descomposición $D_{\mathfrak{P}}(L/K)$.

c) $D_{\mathfrak{P}}(L/K)$ es un subgrupo normal de $G(L/K)$.

Para la demostración de (1.1) se precisará de los siguientes lemas.

Lema (1.2).- Sean A, $\mathfrak{p}$ y K elegidos como en (1.1). Sea L una extensión de K de grado finito y B la clausura entera de A en L. Sea M una extensión separable y finita de K. Si $\mathfrak{p} \in S(M/K)$, para todo divisor primo $\mathfrak{P}$ de $\mathfrak{p}$ en B se verifica que

$$\mathfrak{P} \in S(LM/L).$$

En consecuencia $K_{\mathfrak{p}} \subset L_{\mathfrak{P}}$.

Demostración :

Sea x un elemento primitivo de M/K ; por (I.2.4) el polinomio minimal de x sobre K descompondrá en factores lineales en $\hat{K}_{\mathfrak{p}}$. La extensión LM/L admite a x por elemento primitivo. El polinomio minimal de x sobre L descompondrá en factores lineales en $\hat{L}_{\mathfrak{P}}$. Puesto que x es separable sobre L , aplicando nuevamente (I.2.4) se obtendrá que $\mathfrak{P} \in S(LM/L)$.

Lema (1.3).- Sean A_1 y A_2 anillos de valoración discreta de cuerpo de fracciones K y sean $\mathfrak{p}_1$ y $\mathfrak{p}_2$ sus respectivos ideales maximales. Si $A_1 \neq A_2$, los cuerpos $K_{\mathfrak{p}_1}$ y $K_{\mathfrak{p}_2}$ son también distintos.

Demostración :

Basta construir una extensión separable L de K , de modo que, para cada divisor primo $\mathfrak{P}_{1,i}$ de $\mathfrak{p}_1$ en la clausura entera de A_1 en L se verifique

$$n_{\mathfrak{P}_{1,i}}(L/K) = 1$$

y tal que, exista algún divisor primo $\mathfrak{P}_{2,j}$ de $\mathfrak{p}_2$ en la clausura entera de A_2 en L , para el cual

$$n_{\mathfrak{P}_{2,j}}(L/K) > 1 \ .$$

La existencia de la anterior extensión queda asegurada gracias a un resultado de Krull (véase [23], bastando en el caso de ser K un cuerpo de números [2o]).

Lema (1.4).- Sea A un anillo de valoración discreta, $\mathfrak{p}$ su ideal maximal y K su cuerpo de fracciones. Sea L una extensión finita y galoisiana de K, B la clausura entera de A en L y $\mathfrak{P}$ un divisor primo de $\mathfrak{p}$ en B. Dado $\sigma \in G(L/K)$, la condición necesaria y suficiente para que σ se extienda a un $K_{\mathfrak{p}}$-monomorfismo de $L_{\mathfrak{P}}$ en $\overline{K}$ es que $\sigma \in N_{\mathfrak{p}}(L/K)$.

Demostración :

La necesidad es consecuencia de (I.4.1). Por (1.2) $L_{\mathfrak{P}}$ es extensión de $K_{\mathfrak{p}}$; así para ver el carácter suficiente, dado $\sigma \in N_{\mathfrak{p}}(L/K)$ bastará ascenderlo a un automorfismo de $LK_{\mathfrak{p}}$ que deje fijo $K_{\mathfrak{p}}$. Ya que

$$G(LK_{\mathfrak{p}}/K_{\mathfrak{p}}) \simeq G(L/K_{\mathfrak{p}} \cap L) \quad ,$$

obteniéndose el isomorfismo por restricción a L de los elementos de $G(LK_{\mathfrak{p}}/K_{\mathfrak{p}})$, la posibilidad de extender σ queda probada.

Demostración de (1.1) :

Probaremos primeramente la equivalencia de a) con b). Sea σ un $K_{\mathfrak{p}}$-monomorfismo de $L_{\mathfrak{P}}$ en $\overline{K}$ y sea σ_L su restricción a L. Si $\mathfrak{P}'$ es el divisor primo de B dado por $\sigma_L(\mathfrak{P}) = \mathfrak{P}'$, σ_L es una aplicación uniformemente continua del espacio que se obtiene al dotar a L de la topología $\mathfrak{P}$-ádica en el espacio que se obtiene al dotar a L de la topología $\mathfrak{P}'$-ádica. En consecuencia σ_L se extiende originando un $\hat{K}_{\mathfrak{p}}$-monomorfismo entre los correspondientes completados

$$\sigma_L : \hat{L}_{\mathfrak{p}} \longrightarrow \hat{L}_{\mathfrak{p}'}$$

que es, de hecho, un $\hat{K}_{\mathfrak{p}}$ - isomorfismo (basta contar grados). De ello se deduce que, si $x \in L$, el polinomio minimal de x sobre L descompone en factores lineales en $\hat{L}_{\mathfrak{p}}$ si y sólo si el polinomio minimal de $\sigma(x)$ sobre L descompone linealmente en $\hat{L}_{\mathfrak{p}'}$. En consecuencia,

$$\sigma L_{\mathfrak{p}} = L_{\mathfrak{p}'} .$$

Teniendo en cuenta (1.3), se obtiene ahora

$$\sigma L_{\mathfrak{p}} = L_{\mathfrak{p}} \iff \sigma_L(\mathfrak{p}) = \mathfrak{p} ,$$

con lo cual, se verificará la primera de estas igualdades para todo $K_{\mathfrak{p}}$ - monomorfismo σ de $L_{\mathfrak{p}}$ en $\overline{K}$, si y sólo si $\sigma_L \in D_{\mathfrak{p}}(L/K)$, para todo σ.

La equivalencia de b) y de c) resulta de (1.4).

Observación (1.5).- La equivalencia de a) y de c) en el Teorema (1.1) pone de manifiesto la existencia de extensiones de Galois L/K para las que $L_{\mathfrak{p}}/K_{\mathfrak{p}}$ no es galoisiana. En efecto, si K es un cuerpo de números y G un grupo resoluble finito, existen infinitas extensiones L de K galoisianas y de grupo de Galois G (Shafarevitch [41]). Todo subgrupo cíclico de G es, por el Teorema de Tchebotarev ([26], Cap.VIII, Teor. 1o), grupo de descomposición de infinitos divisores primos $\mathfrak{p}$ de L. Basta entonces elegir un grupo resoluble con subgrupos cíclicos no normales. Por ejemplo, un grupo no abeliano de orden pq, siendo p y q enteros primos distintos. (La construcción efectiva de extensiones de Galois de Q con grupo

de Galois no abeliano de orden pq se ha llevado a cabo en [12]) .

Proposición (1.6).- Sea A un anillo de valoración discreta, $\mathfrak{p}$ su ideal maximal y K su cuerpo de fracciones. Sean L una extensión finita y de Galois de K, B la clausura entera de A en L y $\mathfrak{P}_i$, $1 \leq i \leq g$, los divisores primos de $\mathfrak{p}$ en B. Si $L_{\mathfrak{P}_1,\ldots,\mathfrak{P}_g}$ es el cuerpo totalmente $\mathfrak{p}$-ádico relativo a los ideales $\mathfrak{P}_i$, se verifica :

a) La extensión $L_{\mathfrak{P}_1,\ldots,\mathfrak{P}_g} / K_{\mathfrak{p}}$ es galoisiana.

b) $L_{\mathfrak{P}_1,\ldots,\mathfrak{P}_g} = K_{\mathfrak{p}} \iff \mathfrak{p} \in S(L/K)$.

Demostración :

Probaremos que $L_{\mathfrak{P}_1,\ldots,\mathfrak{P}_g} / K$ es una extensión galoisiana ; puesto que

$$L_{\mathfrak{P}_1,\ldots,\mathfrak{P}_g} \supset K_{\mathfrak{p}} \supset K$$

ello implicará a) .

Sea $x \in L_{\mathfrak{P}_1,\ldots,\mathfrak{P}_g}$ y σ un K-monomorfismo de $L_{\mathfrak{P}_1,\ldots,\mathfrak{P}_g}$ en $\overline{K}$. Representamos también por σ una extensión del monomorfismo anterior a un K-monomorfismo de la composición $L_{\mathfrak{P}_1} \cdot \ldots \cdot L_{\mathfrak{P}_g}$ en $\overline{K}$. A partir de la demostración de (1.1) se obtiene

$$\sigma L_{\mathfrak{P}_1,\ldots,\mathfrak{P}_g} = \bigcap \sigma L_{\mathfrak{P}_i} = \bigcap L_{\sigma(\mathfrak{P}_i)}$$

y puesto que $G(L/K)$ opera en el conjunto de los divisores primos de $\mathfrak{p}$ en B,

$$\bigcap L_{\sigma(\mathfrak{P}_i)} = L_{\mathfrak{P}_1,\ldots,\mathfrak{P}_g} .$$

La demostración de b) es inmediata a partir de las definiciones; en este apartado es suficiente la hipótesis de que L sea una extensión finita de K.

Se demuestra a continuación que las subextensiones de $L_{\mathfrak{P}}$, $L_{\mathfrak{P}} \supset K_{\mathfrak{p}}(x) \supset K_{\mathfrak{p}}$, obtenidas al adjuntar a $K_{\mathfrak{p}}$ un elemento $x \in \bar{K}$, tal que $K(x)/K$ sea una extensión abeliana, tienen grado acotado sobre K. Este resultado será utilizado en el capítulo IV.

<u>Proposición (1.7).-</u> Sea A un anillo de valoración discreta de cuerpo de fracciones K. Sea K^{ab} la extensión abeliana maximal de K, L una extensión separable y finita de K y B la clausura entera de A en L. Para todo ideal primo $\mathfrak{P}$ de B se verifica

$$\left[K_{\mathfrak{p}}(L_{\mathfrak{P}} \cap K^{ab}) : K_{\mathfrak{p}} \right] \leq n_{\mathfrak{P}}(L/K) , \qquad (1)$$

siendo $\mathfrak{p} = \mathfrak{P} \cap A$.

Si L/K es una extensión abeliana, se verifica

$$K_{\mathfrak{p}}(L_{\mathfrak{P}} \cap K^{ab}) = L K_{\mathfrak{p}}$$

siendo válido en este caso en (1), el signo de igualdad.

Demostración :

Sea $x \in L_{\mathfrak{P}}$ un elemento tal que $K(x)/K$ sea de Galois. La extensión $K_{\mathfrak{p}}(x)/K_{\mathfrak{p}}$ será galoisiana y se tendrá

$$G(K_{\mathfrak{p}}(x)/K_{\mathfrak{p}}) \simeq G(K(x)/K(x) \cap K_{\mathfrak{p}}) \simeq N_{\mathfrak{p}}(K(x)/K) ,$$

por (I.4.1). Sea $\bar{\mathfrak{P}}$ un divisor primo de $\mathfrak{P}$ en $L(x)$. Sea $M = K(x)$, C la clausura entera de A en M y $\bar{\mathfrak{p}} = C \cap \bar{\mathfrak{P}}$. Pasando a los correspondientes completados y por ser $x \in L_{\mathfrak{P}}$ se obtiene

$$\hat{K}_{\mathfrak{p}} \subset \hat{M}_{\bar{\mathfrak{p}}} \subset \hat{L}_{\mathfrak{P}} .$$

En consecuencia (y debido a que M/K es de Galois),

$$n_{\mathfrak{p}}(M/K) \leq n_{\mathfrak{P}}(L/K) . \qquad (2)$$

Si $x \in L_{\mathfrak{P}} \cap K^{ab}$, la extensión M/K es abeliana, en consecuencia

$$N_{\mathfrak{p}}(M/K) = D_{\bar{\mathfrak{p}}}(M/K) . \qquad (3)$$

Si por $(N_{\mathfrak{p}}(M/K) : (1))$ indicamos el orden de $N_{\mathfrak{p}}(M/K)$, puesto que

$$\left[M K_{\mathfrak{p}} : K_{\mathfrak{p}} \right] = (N_{\mathfrak{p}}(M/K) : (1))$$

se obtendrá de (2) y de (3) que

$$\left[M K_{\mathfrak{p}} : K_{\mathfrak{p}} \right] \leq n_{\mathfrak{P}}(L/K) .$$

La primera afirmación de la proposición resulta ahora de [25], Cap.VIII, § 1, Lema 1.

Si L/K es una extensión abeliana, basta tener en cuenta que

$$K_{\mathfrak{p}}(L_{\mathfrak{p}} \cap K^{ab}) \supset LK_{\mathfrak{p}}$$

y que el grado de $LK_{\mathfrak{p}}$ sobre $K_{\mathfrak{p}}$ es igual a $n_{\mathfrak{p}}(L/K)$.

2. Infinitud de $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}/K$

Los cuerpos de números y los cuerpos de funciones algebraicas de una variable sobre un cuerpo de constantes finito se designarán, como es habitual, con el nombre de cuerpos globales.

Definición (2.1).- Sea K un cuerpo global. Llamaremos divisores primos de K a las clases de las valoraciones de K no triviales, si K es un cuerpo de números; o bien a las clases de las valoraciones de K no triviales, nulas sobre el cuerpo de constantes de K , si K es un cuerpo de funciones (definiendo como equivalentes aquellas valoraciones con igual anillo de valoración).

Puesto que en ambos casos dichas valoraciones son discretas ([2], Cap.IV, § 4 y [14], Cap.I, § 6), las consideraciones hechas hasta ahora son aplicables.

Si K es un cuerpo de números, los divisores primos de K se corresponden biyectivamente con los ideales primos no nulos del anillo de los enteros de dicho cuerpo. De acuerdo con el § 3 del Capítulo I , en este caso se dispondrá además de los primos infinitos de K .

Divisores primos y primos infinitos serán designados, siempre que no se preste a confusión, con el nombre de primos de K.

Definición (2.2).- Sea K un cuerpo y M una extensión algebraica de K, no necesariamente finita. Definimos el grado $[M:K]$ por

$$[M:K] = \operatorname*{mcm}_{L} [L:K]$$

al recorrer L el conjunto de las subextensiones de M finitas sobre K, e indicando por mcm el mínimo común múltiplo en el sentido de número sobrenatural.

Teorema (2.3).- Sea K un cuerpo global y $\{\mathfrak{p}_i\}_{1\leq i\leq r}$ un conjunto finito de primos de K. Para todo entero primo q, el grado sobre K de la extensión abeliana maximal de K contenida en $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ es divisible por q^{∞}.

Demostración :

Obviamente no es restrictivo el aumentar el número de primos en el conjunto considerado. Sea $C = \{\mathfrak{p}_i\}_{1\leq i\leq r}$ y $\mathfrak{p}_0$ un divisor primo de K no perteneciente a C (posible pues en K el número de divisores primos es infinito).

Por un resultado bien conocido ([1], Cap.X, Teor. 5) dado un conjunto finito C de primos de K y dados números enteros $n_{\mathfrak{p}}$, $\mathfrak{p}\in C$, que sean posibles grados locales, existe una extensión cíclica L de K cuyo grado es el mcm de los $n_{\mathfrak{p}}$ y tal que

$$\left[\hat{L}_{\mathfrak{P}} : \hat{K}_{\mathfrak{p}} \right] = n_{\mathfrak{p}} \quad , \text{ para cada } \quad \mathfrak{p} \in C \, .$$

En nuestro caso bastará seleccionar

$$n_{\mathfrak{P}_o} = q^m \quad \text{y} \quad n_{\mathfrak{P}} = 1 \quad , \text{ para } \quad \mathfrak{P} \in C$$

y construir la correspondiente extensión cíclica L de K de grado q^m, para cada $m \geq 1$.

En el caso de ser K un cuerpo de números, la demostración de que $K_{\mathfrak{P}_1,\ldots,\mathfrak{P}_r} \cap K^{ab}$ es una extensión no finita de K puede hacerse independientemente del resultado de Artin - Tate antes mencionado. Para verlo necesitamos previamente el siguiente

Lema (2.4).- Dado un conjunto finito A de enteros primos, existe siempre un entero $a > o$ no divisible por ningún primo $p \in A$, tal que

$$a \equiv 1 \ (8)$$

$$\left(\frac{a}{p}\right) = +1 \quad , \text{ para todo } \quad p \in A \quad ,$$

indicando $\left(\frac{\ }{\ }\right)$ el símbolo de Legendre.

Demostración :

Sea

$$B = \left\{ p \in A \ ; \ p \equiv 1 \ (4) \right\} \quad \text{y} \quad C = \left\{ p \in A \ ; \ p \equiv 3 \ (4) \right\} .$$

Sin restricción podemos suponer que $B \neq \emptyset$ y $C \neq \emptyset$.

Sea

$$b = \prod_{p \in B} p \quad \text{y} \quad c = \prod_{p \in C} p \quad ,$$

bastará tomar $a = b^2 + c^2 + 7b^2c^2$.

Infinitud de $\left[K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r} \cap K^{ab} : K \right]$, K cuerpo de números.

Sea $C = \{\mathfrak{p}_i\}_{1 \le i \le r}$. Por (I.3.3) podemos suponer que todos los primos infinitos de C son reales. Indiquemos por D el subconjunto de C formado por los divisores primos ; sin restricción podemos suponer $D \neq \emptyset$. Sea

$$A = \left\{ p \in Z \; ; \; (p) = \mathfrak{p} \cap Z \; , \text{ para } \mathfrak{p} \in D \right\} .$$

Con los números primos así obtenidos construyamos un entero $a > o$ verificando las condiciones de (2.4).

Sea

$$m = \prod_{\mathfrak{p} \in D} p \qquad , \text{ tomando } p > o .$$

Al recorrer t todos los enteros positivos, y por ser a y $4m$ primos entre sí, el teorema de Dirichlet ([2], Cap.V, § 3, Teor.2) garantiza la existencia de infinitos enteros primos q_t de la forma

$$q_t = a + t4m .$$

Sea

$$L_t = Q(\sqrt{q_t}) .$$

Según las leyes de descomposición en un cuerpo cuadrático, se tendrá que

L_t / Q ramifica en q_t ,

$p \in S(L_t / Q)$, para todo entero primo $p \mid m$.

Para todos los valores de t considerados, salvo a lo sumo un número finito, se verificará que

$$K \subsetneq KL_t$$

y la extensión KL_t será ramificada en los divisores primos $\mathfrak{q}$ de q_t en K. Por (1.2)

$$\forall \mathfrak{p} \in D \ , \ \mathfrak{p} \in S(KL_t/K) \ .$$

Ya que todo primo real de K descompone también completamente en KL_t, se tendrá

$$KL_t \subset K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r} \cap K^{ab}$$

para los anteriores valores de t. La extensión

$$K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r} \cap K^{ab} / K$$

contendrá infinitos primos ramificados. Es por tanto no finita.

3. Comparación con el HCF

Teorema (3.1).- Sea K un cuerpo de números y K_1 el "Hilbert Class Field" de K, es decir, la extensión abeliana no ramificada maximal de K. Dado un divisor primo $\mathfrak{p}$ de K, se verifica que $K_1 \subset K_{\mathfrak{p}}$ si y sólo si $\mathfrak{p}$ es principal en el anillo de los enteros A_K de K.

Demostración :

Sea $(\mathfrak{p}, K_1/K)$ el símbolo de Artin de $\mathfrak{p}$ ([39], Cap.I, § 8). Su orden es igual al grado residual $f_{\mathfrak{p}}(K_1/K)$.

En consecuencia

$$\mathfrak{p} \in S(K_1/K) \iff (\mathfrak{p}, K_1/K) = Id.$$

Indiquemos por I_K el grupo de los divisores de K y por P_K el subgrupo de I_K formado por los divisores principales. En virtud de la ley de reciprocidad de Artin ([26], Cap.XI, § 5), se tiene

$$I_K/P_K \cong G(K_1/K)$$

viniendo dado el isomorfismo anterior por

$$\alpha = \prod \mathfrak{p}^{\nu_\mathfrak{p}} \longrightarrow (\alpha, K_1/K) = \prod (\mathfrak{p}, K_1/K)^{\nu_\mathfrak{p}},$$

para $\alpha \in I_K$.

En consecuencia

$$(\mathfrak{p}, K_1/K) = Id \iff \mathfrak{p} \in P_K, \quad \text{c.q.d.}$$

Sea $K_o = K$ y K_i el Hilbert Class Field de K_{i-1}, para $i \geq 1$. Al considerar la torre de HCF de K

$$K = K_o \subset K_1 \subset \dots \subset K_r \subset \dots$$

(posiblemente infinita según el Teorema de Golod - Shafarevitch [18], o bien [9], exp.IX), se obtiene el siguiente

Corolario (3.2).- Sea $\mathfrak{p}_r$ un divisor primo de K_r y $\mathfrak{p}_i$ su restricción a K_i, para $o \leq i < r$. La condición necesaria y suficiente para que $K_r \subset K_\mathfrak{p}$ es que $\mathfrak{p}_i$ sea principal en K_i, para $o \leq i \leq r-1$.

Demostración :

Basta tener en cuenta que, por ser K_r / K una extensión galoisiana

$$\mathfrak{p} \in S(K_r/K) \iff \mathfrak{p}_i \in S(K_{i+1}/K_i) \text{ , para } o \leq i < r$$

y aplicar (3.1) .

Capítulo III

GRUPO DE BRAUER

Introducción.

Dado un cuerpo global K y un primo p del mismo, se relaciona el grupo de Brauer de K_p con el de $\hat{K}_p$. Un estudio de la sucesión espectral de Hochschild-Serre permite obtener que $B(\hat{K}_p)$ es isomorfo al subgrupo de $B(K_p)$ fijo por la acción de $G(K_p/K)$.

En el caso de partir de un conjunto finito de primos, el subgrupo análogo al anterior en $B(K_{p_1,\dots,p_r})$ es isomorfo a $B(\hat{K}_{p_1}) \times \dots \times B(\hat{K}_{p_r})$.

La información obtenida acerca del grupo de Brauer permite afirmar que los cuerpos $K_{p_1,\dots,p_r}$ (salvo en el caso en que $K_{p_1,\dots,p_r} = \overline{K}$) no son C_1 , resultado de interés antes de emprender un estudio diofántico de los mismos.

En el capítulo I se ha obtenido el grupo de Galois $G(\overline{K}/K_p)$ como límite proyectivo de los grupos $N_p(L/K)$. Es sabido que los grupos de descomposición son resolubles ; al pasar a los subgrupos normales que ellos generan, éstos pueden dejar de serlo. En el caso de ser K un cuerpo de números se obtiene que, efectivamente, $G(\overline{K}/K_p)$ es un grupo de Galois no pro-resoluble. Se llega a este resultado a

través del grupo de Brauer de K_p y en particular permite deducir, para todo cuerpo de números K y para todo conjunto finito $p_1,\dots,p_r$ de primos de K, la existencia de una extensión galoisiana L de K en la que los grupos $N_{p_i}(L/K)$, $1 \leq i \leq r$, no son resolubles.

Por último, el conocimiento de que las p-componentes de $B(K_p)$ no son nulas se aplica a la determinación de la dimensión cohomológica de K_p .

1. Consideraciones previas

Dado un grupo compacto totalmente discontínuo G y un G-módulo topológico discreto A , por $H^q(G,A)$, para $q \geq o$, se representan los grupos de cohomología ordinarios de G a coeficientes en A ; es decir

$$H^q(G,A) = Ext_C^q(Z,A)$$

siendo $Ext_C^q(Z,A)$ el q-ésimo functor derivado del functor $A \rightsquigarrow A^G = Hom_G(Z,A)$.

$\{ H^n(G,-), \delta \}$ constituye un functor cohomológico. En consecuencia, a todo homomorfismo continuo

$$f : G' \longrightarrow G$$

corresponde un homomorfismo de functores cohomológicos $\{ f_q^* \}$,

$$f_q^* : H^q(G,A) \longrightarrow H^q(G',A)$$

que se obtiene de la prolongación del homomorfismo natural

$$f_o^* : A^G \longrightarrow A^{G'} \quad .$$

En particular, si H es un subgrupo normal y cerrado de G y B es un G/H-módulo topológico discreto, se obtienen los homomorfismos

$$\text{res} : H^*(G,A) \longrightarrow H^*(H,A)$$

$$\text{inf} : H^*(G/H,B) \longrightarrow H^*(G,B)$$

de restricción y de inflación, respectivamente.

El estudio de la cohomología de un grupo compacto totalmente discontínuo se reduce, gracias al empleo de cocadenas contínuas, al de la cohomología de los grupos finitos a través de la relación

$$H^*(G,A) = \varinjlim H^*(G/H, A^H)$$

obtenida al recorrer H el conjunto de los subgrupos de G normales y abiertos y siendo los morfismos los de inflación.

Si H es un subgrupo normal y cerrado de G y A es un G-módulo topológico discreto, G/H opera en $H^q(H,A)$. Si $f(\sigma_1,\ldots,\sigma_q)$ es un cociclo, $\tau \in G$ y $\overline{\tau}$ es su imagen en G/H, basta definir como representante de la clase imagen de la de f

$$(\overline{\tau} f)(\sigma_1,\ldots,\sigma_q) = \tau f(\tau^{-1}\sigma_1\tau, \ldots, \tau^{-1}\sigma_q\tau) \quad .$$

La anterior operación convierte a $H^q(H,A)$ es un G/H-módulo topológico discreto. Pueden por tanto considerarse los grupos de cohomología $H^p(G/H, H^q(H,A))$.

La sucesión espectral de extensiones de grupos (Hochschild - Serre),

$$H^p(G/_H, H^q(H,A)) \underset{p}{\Longrightarrow} H^*(G,A) \quad ,$$

permite obtener, dado un G-módulo tal que

$$H^i(H,A) = o \quad , \text{ para } 1 \leq i \leq q-1 \quad ,$$

la sucesión exacta

$$o \longrightarrow H^q(G/_H, A^H) \xrightarrow{inf} H^q(G,A) \xrightarrow{res} H^q(H,A)^{G/H} \longrightarrow$$

$$\xrightarrow{tg} H^{q+1}(G/_H, A^H) \xrightarrow{inf} H^{q+1}(G,A) \quad ,$$

siendo tg el morfismo de transgresión ([22] y [42], Cap.II, § 4).

2. Relación del grupo de Brauer de $K_\mathfrak{p}$ con el de $\hat{K}_\mathfrak{p}$

Dado un cuerpo K se indica por $B(K)$ su grupo de Brauer. Como es sabido, si $\overline{K}$ es una clausura separable de K, el segundo grupo de cohomología de $G(\overline{K}/K)$ a valores en el grupo multiplicativo $\overline{K}^*$ coincide con $B(K)$:

$$B(K) = H^2(G(\overline{K}/K), \overline{K}^*)$$

([39], Cap.X, §§ 4,5) .

Lema (2.1).- Sea K un cuerpo global, $\mathfrak{p}$ un primo de K y $K_\mathfrak{p}$ el cuerpo totalmente $\mathfrak{p}$-ádico relativo a $\mathfrak{p}$. El grupo de Brauer $B(K_\mathfrak{p})$ tiene estructura de $G(K_\mathfrak{p}/K)$-módulo. El subgrupo de $B(K_\mathfrak{p})$ fijo por la acción de $G(K_\mathfrak{p}/K)$ se incluye en la siguiente sucesión exacta :

$$o \longrightarrow H^2(G(K_\mathfrak{p}/K), K_\mathfrak{p}^*) \xrightarrow{inf} B(K) \xrightarrow{res} B(K_\mathfrak{p})^{G(K_\mathfrak{p}/K)} \longrightarrow o \, .$$

Demostración :

Sea $G = G(\overline{K}/K)$, dotado de la topología de Krull y sea $H = G(\overline{K}/K_{\mathfrak{p}})$. Puesto que H es un subgrupo cerrado de G y normal, la primera de las afirmaciones resulta de hacer operar el cociente $G/_H$ en

$$H^2(G(\overline{K}/K_{\mathfrak{p}}) , \overline{K}^*) = B(K_{\mathfrak{p}})$$

según se ha indicado en el §1 .

Al recorrer L el conjunto de las extensiones finitas y galoisianas de K contenidas en $\overline{K}$, del Teorema 9o de Hilbert, resulta

$$H^1(G,\overline{K}^*) = \varinjlim_{L} H^1(G(L/K) , L^*) = o \ .$$

En consecuencia, la sucesión de Hochschild - Serre proporcionará, para $q = 2$, la sucesión exacta siguiente :

$$o \longrightarrow H^2(G(K_{\mathfrak{p}}/K) , K_{\mathfrak{p}}^*) \longrightarrow B(K) \longrightarrow$$

$$\longrightarrow B(K_{\mathfrak{p}})^{G(K_{\mathfrak{p}}/K)} \longrightarrow H^3(G(K_{\mathfrak{p}}/K) , K_{\mathfrak{p}}^*) \ .$$

Probaremos a continuación que $H^3(G(K_{\mathfrak{p}}/K) , K_{\mathfrak{p}}^*) = o$.

Al recorrer L el conjunto de las extensiones finitas y galoisianas de K contenidas en $K_{\mathfrak{p}}$ se obtiene

$$H^3(G(K_{\mathfrak{p}}/K) , K_{\mathfrak{p}}^*) = \varinjlim_{L} H^3(G(L/K) , L^*) \ .$$

Para cada L , $H^3(G(L/K) , L^*)$ es un grupo cíclico generado por el cociclo de Teichmüller $t_{L/K}$ ([1], Cap.VII) . La demostración consistirá en probar que, para cada $L \subset K_{\mathfrak{p}}$

podemos construir una extensión M galoisiana sobre K, de modo que

$$K_{\mathfrak{p}} \supset M \supset L \supset K$$

e $\inf_M t_{L/K} = o$.

Sean J_L y C_L los grupos de ideles y de clases de ideles, respectivamente, de L . Consideremos la sucesión exacta

$$1 \longrightarrow L^* \longrightarrow J_L \longrightarrow C_L \longrightarrow 1$$

que se obtiene al proyectar J_L en C_L . La sucesión exacta de cohomología proporciona la siguiente sucesión exacta

$$H^2(G(L/K), J_L) \longrightarrow H^2(G(L/K), C_L) \xrightarrow{\delta}$$

$$\longrightarrow H^3(G(L/K), L^*) \longrightarrow H^3(G(L/K), J_L) ,$$

siendo $H^3(G(L/K), J_L) = o$, en virtud del Lema de Shapiro ([48], Cap.III) y de la teoría local de cuerpos de clases ([39], Cap.XIII) .

Si M es una extensión de L galoisiana sobre K , por ser la inflación un morfismo de functores cohomológicos, el siguiente diagrama es conmutativo

$$\begin{array}{ccc} H^2(G(M/K), C_M) & \xrightarrow{\delta_M} & H^3(G(M/K), M^*) \\ \text{inf.}\uparrow & & \text{inf.}\uparrow \\ H^2(G(L/K), C_L) & \xrightarrow{\delta_L} & H^3(G(L/K), L^*) \end{array} .$$

El cociclo de Teichmüller $t_{L/K}$ se obtiene como imagen

por δ de la clase fundamental $c_{L/K}$ de $H^2(G(L/K), C_L)$ (por la teoría global de cuerpos de clases, este último es un grupo cíclico de orden $n = [L : K]$ generado por un elemento, $c_{L/K}$, de invariante de Hasse igual a $1/n$ ([1], Cap.VII)). Bastará por tanto construir M de modo que

$$\inf_M c_{L/K} \in \ker \delta_M .$$

Como es sabido ([1], Cap.VII, Teor.11), el $\ker \delta_M$ lo constituyen los elementos $c \in H^2(G(M/K), C_M)$ de invariante r/m, en donde r es un entero y m es el mínimo común múltiplo de los grados locales $n_q(M/K)$ obtenidos al recorrer q todos los primos de K.

Sea q un divisor primo de K, $q \neq p$. Por [1], Cap.X, Teor.5, existe una extensión galoisiana M_o/K de grado $n = [L : K]$, tal que

$$n_p(M_o/K) = 1 \quad , \quad n_q(M_o/K) = n .$$

Pongamos $M = M_o L$. La extensión M/K será galoisiana y por (I.2.2) o por su análogo en el caso no ultramétrico, M será un subcuerpo de K_p; el mínimo común múltiplo de los grados locales de M/K será divisible por n. Teniendo en cuenta que el invariante no es alterado por la inflación ([1], Cap.VII, § 3, Lema 1), se tendrá

$$\operatorname{inv} \inf_M c_{L/K} = \operatorname{inv} c_{L/K} = \frac{1}{n} \quad ;$$

en consecuencia, $\inf_M c_{L/K} \in \ker \delta_M$. Ello concluye la demostración.

Teorema (2.2).- Sea K un cuerpo global y p un pri-

mo de K . El subgrupo de $B(K_\mathfrak{p})$ fijo por $G(K_\mathfrak{p}/K)$ es isomorfo al grupo de Brauer del completado de K en $\mathfrak{p}$.

En consecuencia se obtiene :

$$B(K_\mathfrak{p})^{G(K_\mathfrak{p}/K)} \simeq Q/Z \qquad \text{si } \mathfrak{p} \text{ es un divisor primo}$$

$$B(K_\mathfrak{p})^{G(K_\mathfrak{p}/K)} \simeq Z/(2) \qquad \text{si } \mathfrak{p} \text{ es un primo real}$$

$$B(K_\mathfrak{p}) = o \qquad \text{si } \mathfrak{p} \text{ es un primo complejo .}$$

Demostración :

Debido a la sucesión exacta de (2.1) bastará estudiar el cociente de $B(K)$ por $\inf H^2(G(K_\mathfrak{p}/K), K_\mathfrak{p}^*)$.

Sea $\mathfrak{q}$ un primo de K y A un álgebra simple de centro K y de rango finito sobre este cuerpo. La aplicación

$$A \longrightarrow A \underset{K}{\otimes} \hat{K}_\mathfrak{q}$$

origina un morfismo de $B(K)$ en $B(\hat{K}_\mathfrak{q})$. Al tener en cuenta todos los valores absolutos de K se tiene un monomorfismo

$$B(K) \longrightarrow \bigoplus_{\mathfrak{q}} B(\hat{K}_\mathfrak{q})$$

([1], Cap.VI, Teor.2) ; otras demostraciones se encuentran en [47], o en [13].

De [1], Cap.VII, Teor.8 y Cap.X, Teor.5 , se deduce que el monomorfismo anterior se incluye en una sucesión exacta

$$o \longrightarrow B(K) \longrightarrow \bigoplus_{\mathfrak{q}} B(\hat{K}_\mathfrak{q}) \xrightarrow{\text{inv}} Q/Z \longrightarrow o \ ,$$

en donde la aplicación invariante viene dada mediante los

invariantes locales por

$$\text{inv}\,((c_q)) = \sum \text{inv}_q\, c_q \ .$$

Sea P el conjunto de los divisores primos de K y P_∞ el de los primos de K reales. Puesto que

$$B(\hat{K}_q) \simeq Q/Z \qquad , \text{ si } q \in P$$

$$B(\hat{K}_q) = B(R) \simeq Z/(2) \qquad , \text{ si } q \in P_\infty$$

([39] , Cap.XIII, § 3 y Cap.X , § 7) y todo cuerpo algebraicamente cerrado tiene grupo de Brauer nulo, el grupo de Brauer de K es isomorfo a B siendo

$$B = \left\{ (x_q) \in \left(\bigoplus_{q \in P} (Q/Z)_q \right) \oplus \left(\bigoplus_{q \in P_\infty} (Z/(2))_q \right) \ ; \sum x_q = 0 \right\}.$$

Sea C el subgrupo de B correspondiente a $\inf H^2(G(K_p/K) , K_p^*)$ en el isomorfismo anterior. Probaremos que C es el subgrupo de B formado por aquellos elementos que tienen nula la componente p-ésima.

Sea $c \in B(K)$ un elemento que pertenezca a la imagen de inf . Existirá una extensión L finita y galoisiana de K tal que

$$K_p \supset L \supset K$$

e $\inf d = c$, para cierto $d \in H^2(G(L/K) , L^*)$.

Puesto que $n_p(L/K) = 1$, se tendrá

$$\mathrm{inv}_p d = o$$

y, en consecuencia, la imagen de c en B tendrá nula la componente correspondiente a p . Recíprocamente, si $(x_q) \in B$ es un elemento tal que $x_p = o$, por [1], Cap.VII, Teor. 8 y Cap.X, Teor. 5 , se podrá obtener una extensión finita y de Galois de K , L , contenida en K_p y un cociclo

$$e \in H^2(G(L/K), L^*)$$

de modo que

$$(\mathrm{inv}_q(e)) = (x_q) .$$

A la vista de (2.1) se obtienen ahora los siguientes isomorfismos

$$B(K_p)^{G(K_p/K)} \simeq \frac{B(K)}{\inf H^2(G(K_p/K), K_p^*)} \simeq B/c \simeq B(\hat{K}_p)$$

correspondientes a las aplicaciones $\overline{\mathrm{res}}^{-1}$, $\overline{\mathrm{inv}}$ e inv_p^{-1} , respectivamente . Con ello se llega al resultado requerido.

Teorema (2.2').- Sea K un cuerpo global y

$\{\mathfrak{P}_i\}_{1 \leq i \leq r}$ un conjunto finito de primos de K. El grupo de Brauer $B(K_{\mathfrak{P}_1,\ldots,\mathfrak{P}_r})$ tiene estructura de $G(K_{\mathfrak{P}_1,\ldots,\mathfrak{P}_r}/K)$ - módulo y se verifica

$$B(K_{\mathfrak{P}_1,\ldots,\mathfrak{P}_r})^{G(K_{\mathfrak{P}_1,\ldots,\mathfrak{P}_r}/K)} \simeq B(\hat{K}_{\mathfrak{P}_1}) \times \ldots \times B(\hat{K}_{\mathfrak{P}_r}) .$$

Demostración :

Basta tener en cuenta que todos los pasos de (2.1) y de (2.2) se pueden efectuar de manera análoga cuando, en lugar de un único primo de K, se consideran un número finito.

3. Consecuencias

Definición (3.1).- Un cuerpo K se dice que es C_r, si todo polinomio homogéneo $F(X_1, \ldots, X_n)$ a coeficientes en K, cuyo grado d sea tal que $n > d^r$, tiene un cero no trivial en K^n.

Un cuerpo K es C_o si y sólo si es algebraicamente cerrado.

Los cuerpos C_1 son llamados también cuerpos casi algebraicamente cerrados.

Proposición (3.2).- Sea K un cuerpo global y

$K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ un cuerpo totalmente $\mathfrak{p}$-ádico construido a partir de K . Las siguientes afirmaciones son equivalentes :

a) $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ es casi algebraicamente cerrado.

b) K es un cuerpo de números y todos los primos $\mathfrak{p}_i$ son complejos.

c) $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ es algebraicamente cerrado.

Demostración :

Si $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ es C_1 , su grupo de Brauer debe ser cero ([39], Cap.X, Prop. 1o) . Por (2.2') se sigue que $B(\hat{K}_{\mathfrak{p}_i}) = o$, para $1 \leq i \leq r$, lo cual obliga a que cada $\mathfrak{p}_i$ sea un primo complejo, y en particular, a que K sea un cuerpo de números. En consecuencia a) $\Longrightarrow$ b)

Para ver que b) $\Longrightarrow$ c) basta tener en cuenta que bajo las hipótesis de b) , es $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r} = \overline{K}$.

La implicación c) $\Longrightarrow$ a) es trivial .

Observación (3.3).- Si K es un cuerpo global de funciones, los teoremas de Chevalley y de Tsen ([19], Cap.II y Cap.III) permiten deducir que los cuerpos $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ son C_2 .

En el caso de que $K = Q$, el ejemplo de Terjanian para $p = 2$, y los ejemplos de Schanuel para un primo p cualquiera , para probar que el cuerpo p-ádico $\hat{Q}_p$ no es C_2 ([19] , Cap. VII) , sirven para poner de manifiesto que los cuerpos $Q_{p_1,\ldots,p_r}$ no son C_2 . Basta tener en cuenta que dichos ejemplos se fabrican con formas a coeficientes racionales.

En la demostración de la proposición siguiente será necesario el concepto de cuerpo henseliano. Precisamos a continuación su definición.

Definición (3.4).- Un cuerpo K se denomina henseliano (respectivamente antihenseliano) cuando posee un valor absoluto f tal que , para toda extensión finita y separable L de K , el número de extensiones de f a L , salvo equivalencias, es igual a 1 (respectivamente es > 1) .

Proposición (3.5).- Sea K un cuerpo de números y $P = \{p_i\}_{1 \leq i \leq r}$ un conjunto de primos de K , no todos infinitos . El grupo de Galois $G(\overline{K}/K_{p_1,\ldots,p_r})$ no es pro-resoluble .

Demostración :

De (2.2′) se sigue que el grupo de Brauer

$B(K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r})$ no es un p-grupo ni un $\{2,3\}$-grupo. Si $G(\overline{K}/K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r})$ fuera pro-resoluble, se seguiría ([28], Teor. 1) que $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ debería ser un cuerpo henseliano. (Esta misma afirmación podría obtenerse a partir de [28], Teor. I, sin hacer uso de (2.2'), teniendo en cuenta que si $\mathfrak{p} \in P$, $\hat{K}_{\mathfrak{p}}$ puede identificarse al completado de $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ por un valor absoluto extendiendo el definido en K por $\mathfrak{p}$ y que si $\mathfrak{p}$ es finito, $B(\hat{K}_{\mathfrak{p}})$ es isomorfo a Q/Z).

Veremos a continuación que $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ no es henseliano. Supongamos que f fuera un valor absoluto de $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ para el cual fuera henseliano.

Ya que $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ no es algebraicamente cerrado, f no puede ser un valor absoluto no ultramétrico complejo.

Si f fuera un valor absoluto no ultramétrico real, el grado de $\overline{K}/K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ debería ser 2 ([16], Cap. IV, 26.9). Ello no es posible; en efecto, sea $q \neq 2$ un entero primo, $\mathfrak{p} \in P$ un divisor primo y L una extensión cíclica de K de grado q para la cual $\mathfrak{p} \notin S(L/K)$.

Bajo estas condiciones,

$$\left[L\,K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r} : K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r} \right] = q .$$

Supongamos f ultramétrico y que la clase definida por la restricción de f a K, $\mathfrak{p}$, perteneciera a P. Ya que el cuerpo residual de f es ahora finito, $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ sería un cuerpo local de números algébricos en el sentido de Neukirch ([29], § 3). Al contar los grados locales se obtiene que debería coincidir con un cuerpo local minimal sobre K. Ello obligaría a que $r = 1$, es decir, a que

$$K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r} = K_{\mathfrak{p}} .$$

Representemos por $\bar{f}$ una extensión de f a $\bar{K}$ y por $\bar{\mathfrak{p}}$ la clase de $\bar{f}$. Sea $K_{\bar{\mathfrak{p}}}$ el mínimo cuerpo local sobre K correspondiente a $\bar{\mathfrak{p}}$. Para toda extensión finita y de Galois L de K, tendríamos

$$G(L/L\cap K_{\bar{\mathfrak{p}}}) = D_{\mathfrak{p}}(L/K)$$

en donde $\mathfrak{p}$ es el divisor primo de L obtenido por la restricción a L de $\bar{\mathfrak{p}}$. Puesto que es siempre posible construir extensiones galoisianas L de K en las que

$$D_{\mathfrak{p}}(L/K) \neq N_{\mathfrak{p}}(L/K)$$

(véase (II.1.5)), de (I.4.1) se sigue que $K_{\bar{\mathfrak{p}}} \neq K_{\mathfrak{p}}$,

con lo cual este caso tampoco puede presentarse.

Supongamos por último que $\mathfrak{p} \notin P$. Los valores absolutos de $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ que extienden los valores absolutos de K definidos por los $\mathfrak{p}_i \in P$ deberían ser antihenselianos ([16], Cap. IV , 26.5) . Pero ello no es posible, pues uno al menos de los valores absolutos está, por hipótesis, asociado a una valoración discreta y una valoración discreta no es nunca antihenseliana (basta para verlo tomar un polinomio de Eisenstein) .

Corolario (3.6).- Dado un cuerpo de números K y un conjunto finito P de divisores primos de K , existe una extensión finita y de Galois L de K tal que , para cada $\mathfrak{p} \in P$, el grupo $N_{\mathfrak{p}}(L/K)$ no es resoluble.

Demostración :

Dado $\mathfrak{p} \in P$, por (3.5) podemos elegir un elemento $x \in \overline{K}$ de modo que $K_{\mathfrak{p}}(x)/K_{\mathfrak{p}}$ sea una extensión de Galois no resoluble . Sea $K(y)$ la clausura galoisiana de $K(x)$ sobre K . La extensión $K_{\mathfrak{p}}(y)/K_{\mathfrak{p}}$ será galoisiana no resoluble . Puesto que

$$G(K_{\mathfrak{p}}(y)/K_{\mathfrak{p}}) \simeq G(K(y)/K(y)\cap K_{\mathfrak{p}}) = N_{\mathfrak{p}}(K(y)/K)$$

por (I.4.1) , este último será un grupo no resoluble.

Para cada $\mathfrak{p}_i \in P$, sea $K(y_i)$ una extensión de K obtenida por el procedimiento anterior. Si designamos por r el número de elementos de P , la extensión

$$L = K(y_1,\dots,y_r)$$

cumplirá los requisitos del enunciado.

4. Dimensión cohomológica de $K_{\mathfrak{p}_1,\dots,\mathfrak{p}_r}$

Proposición (4.1).- Sea K un cuerpo global , $\overline{K}$ una clausura separable de K , $\{\mathfrak{p}_i\}_{1\leq i\leq r}$ un conjunto de primos de K no todos infinitos y $G = G(\overline{K}/K_{\mathfrak{p}_1,\dots,\mathfrak{p}_r})$. Dado un entero primo p , sea $cd_p G$ la p-dimensión cohomológica de G . Se verifica :

a) Si $p \neq 2$, $cd_p G = 2$.
Si $p = 2$, $cd_2 G \geq 2$.

b) Si K es un cuerpo de funciones , o bien un cuerpo de números totalmente imaginario,

$$cd_p G = 2 \text{ , para todo } p .$$

Demostración :

Puesto que G es un subgrupo cerrado de $G(\overline{K}/K)$, para todo p se tendrá

$$cd_p G \leq cd_p G(\overline{K}/K) .$$

Si K es un cuerpo de funciones de una variable sobre

un cuerpo finito se verifica ([38], Cap.II, § 4)

$$cd_p\, G(\overline{K}/K) \leq 2 \quad , \text{ para todo } p .$$

Desigualdad análoga a la anterior es válida si K es un cuerpo de números totalmente imaginario, o bien si siendo K un cuerpo de números es $p \neq 2$ ([38], Cap.II, § 4, Prop.13).

Ya que $\overline{K}^*$ es un grupo p-divisible, si $cd_p\, G \leq n$ la componente p-primaria de $H^q(G,\overline{K}^*)$ debe ser nula para todo $q > n$ ([38], Cap.I, § 3, Prop.12). El teorema (2.2′) permite afirmar que

$$cd_p\, G \geq 2$$

en todos los casos.

Capítulo IV

ECUACIONES DIOFANTICAS RESOLUBLES EN K_p

Introducción.

Un teorema de Peck [3o] afirma que, dado un cuerpo de números K y un entero positivo impar n, existe una constante $c(n,K)$ tal que, para todo entero $m > c(n,K)$, toda forma diagonal

$$a_1 X_1^n + \dots + a_m X_m^n$$

en la que los $a_i \in K^*$, tiene un cero no trivial en K. El valor de la constante de Peck de K es

$$c(n,K) = 1 + \max (4n^{2r+3} , (2^{n-1} + r)\, nr) .$$

siendo $r = \left[K : Q \right]$.

Dado un divisor primo p de K, se determinan en este capítulo ciertos valores de n, para los cuales existe una constante $c(n,K,p)$, tal que, para todo $m > c(n,K,p)$, las formas anteriores representan cero en K_p. Sobre la paridad de n no se hace hipótesis alguna. En los casos en que n es impar, el valor obtenido para la constante es

$$c(n,K,p) = n^2 q^{v_p(n)} \leq n^{r+2}$$

indicando q el número de elementos del cuerpo residual de $\hat{K}_p$.

El resultado anterior se obtiene, siguiendo una idea de

Brauer [7] , a partir del estudio del índice de K_p^{*n} en K_p^* . Dicho estudio se efectúa sobre la base de un cuerpo global K arbitrario.

El hecho de que si K es un cuerpo de funciones, K_p sea un cuerpo C_2 , o bien el de que si K es un cuerpo de números y p un primo infinito, K_p sea un cuerpo pitagórico, permite disponer en estos casos de un sistema de invariantes para la clasificación de las formas cuadráticas definidas en K_p.

1. Raíces n-ésimas. Formas diagonales

Proposición (1.1).- Sea K un cuerpo global , p un divisor primo de K y $q = p^f$ el número de elementos del cuerpo residual de $\hat{K}_p$. Se verifica :

a) Si $n \geq 1$ es un entero no divisible por p y $\varepsilon_n \in \overline{K}$ es una raíz primitiva n-ésima de la unidad ,

$$\varepsilon_n \in K_p \iff n \mid q-1 \ .$$

b) Si K es un cuerpo de números y $n = p^s$, $s \geq 1$,

$$\varepsilon_{p^s} \in K_p \implies \varphi(p^s) \leq n_p(K/Q) \ ,$$

siendo φ en indicador de Euler.

Demostración :

Si $p \nmid n$, la extensión $K(\varepsilon_n)/K$ es no ramificada

en $\mathfrak{p}$ y el grado residual $f_{\mathfrak{p}}(K(\varepsilon_n)/K)$ se caracteriza como el menor entero $r \geq 1$ tal que

$$q^r \equiv 1 \ (n) \ .$$

De ello se deduce a) .

Supongamos que K es un cuerpo de números y que $\varepsilon_{p^s} \in K_{\mathfrak{p}}$. Teniendo en cuenta las reglas de descomposición en los cuerpos ciclotómicos, (I.4.1) y (II.1.7) y puesto que $Q(\varepsilon_n)/Q$ es una extensión abeliana, se deduce

$$\varphi(p^s) = n_p(Q(\varepsilon_{p^s})/Q) = \left[Q_p(\varepsilon_{p^s}) : Q_p \right] \leq n_{\mathfrak{p}}(K/Q) \ .$$

<u>Corolario (1.2).-</u> Dado un cuerpo de números K , para toda elección finita de divisores primos de K , el número de raíces de la unidad contenidas en $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ es finito.

<u>Teorema (1.3).-</u> Sea K un cuerpo global, $\mathfrak{p}$ un divisor primo de K y $q = p^f$ el número de elementos del cuerpo residual de $\hat{K}_{\mathfrak{p}}$. Sea W una clausura algebraica de $\hat{K}_{\mathfrak{p}}$ y

$$h : \overline{K} \longrightarrow W$$

un K-monomorfismo.

Dado un entero $n \geq 1$ no divisible por la característica de K , se verifica :

a) Si las raíces n-ésimas de la unidad están contenidas en $\hat{K}_{\mathfrak{p}}$

$$K_{\mathfrak{p}}^{*n} \cap K = h^{-1}(\hat{K}_{\mathfrak{p}}^{*n}) \cap K \ .$$

b) Si $n = t^s$, $s \geq 1$, siendo t un entero primo distinto de p y $t \nmid q-1$

$$K_p^{*n} \cap K \subsetneq h^{-1}(\hat{K}_p^{*n}) \cap K \quad .$$

Demostración :

La inclusión $K_p^{*n} \subset h^{-1}(\hat{K}_p^{*n})$ resulta de (I.2.4) y es válida sin restricción alguna sobre n .

Sea $x \in h^{-1}(\hat{K}_p^{*n}) \cap K$, e $y_o \in \hat{K}_p$ un elemento tal que

$$h(x) = y_o^n \quad ;$$

y_o será algebraico sobre $h(K)$; puesto que $h(K) \subset h(\overline{K})$ y este último es un cuerpo algebraicamente cerrado, se sigue que

$$y_o \in h(\overline{K}) \quad .$$

Sea $y \in \overline{K}$ un elemento tal que $h(y) = y_o$. El elemento y hallado es raíz de la ecuación

$$X^n - x = 0$$

definida en K . Bastará ver bajo qué condiciones

$$p \in S(K(y)/K) \quad .$$

Si las raíces n-ésimas de la unidad están contenidas en $\hat{K}_p$, el polinomio $X^n - h(x)$ descompone en $\hat{K}_p$ en producto de factores lineales. Por tanto, por (I.2.4),

$$y \in K_p \quad .$$

Si $p \neq t$ y $t \nmid q-1$, las raíces t-ésimas de la unidad no están contenidas en $\hat{K}_p$; por tanto, si $n = t^s$, siendo t primo, el elemento $y_o \in \hat{K}_p$ elegido de modo que $h(x) = y_o^n$ es único y en consecuencia, también será único el elemento $y \in \overline{K}$ construido de forma que

$$x = y^n \qquad y \qquad h(y) \in \hat{K}_p \ .$$

Con lo cual, para probar que $x \notin K_p^{*n}$, para ciertos elementos

$$x \in h^{-1}(\hat{K}_p^{*n}) \cap K \ ,$$

bastará probar que $y \notin K_p$. Tomemos x verificando

$$x \in h^{-1}(\hat{K}_p^{*n}) \cap K \qquad y \qquad x \notin K^{*t} \ ;$$

la existencia de tales elementos será probada en los lemas (1.4) y (1.5) que se darán a continuación. Si t es además impar, el polinomio

$$X^n - x$$

es entonces irreducible en K ([3], Cap. V, § 11, ejer.12, o bien [25], Cap. VIII, § 9, Cor.1). Por tanto, si se elige y como en el caso anterior y $\varepsilon_n \in \overline{K}$ es una raíz primitiva n-ésima de la unidad, $K(y, \varepsilon_n)$ será la clausura galoisiana de $K(y)$ sobre K. Bajo las condiciones de b), (1.1) permite afirmar que

$$\varepsilon_n \notin K_p \ .$$

En consecuencia

$$\mathfrak{p} \notin S(K(y,\varepsilon_n)/K) \ .$$

Debido a que las condiciones de b) obligan a que t sea impar y puesto que el que $\mathfrak{p}$ descomponga completamente en $K(y)$ es una condición sobre todos los conjugados de y sobre K,

$$\mathfrak{p} \notin S(K(y)/K) \ .$$

Ello prueba b) .

De la demostración anterior se deduce a su vez que

$$K_{\mathfrak{p}}^{*t} \cap K = K^{*t} \ .$$

Este resultado se ampliará en el apartado siguiente.

Nota.- El ejercicio de Bourbaki citado en la anterior demostración es la exposición de un trabajo de A.Capelli, [8]. Este trabajo ha sido generalizado recientemente por A.Schinzel, [35]

La demostración de (1.3) concluye con el lema (1.5) que se da a continuación; previamente se precisa del siguiente resultado.

Lema (1.4).- Si K es el cuerpo de fracciones de un anillo de Dedekid A que posee infinitos ideales primos, para todo entero $n > 1$, el índice

$$(K^* : K^{*n})$$

es infinito.

Demostración :

Supongamos que $(K^* : K^{*n}) < \infty$. Sea $a_1,\dots,a_m$ un sistema completo de representantes de K^*/K^{*n} .

Dado $a \in K^*$ existe un a_i y un elemento $b \in K^*$ tales que

$$a = a_i b^n .$$

Para todo ideal primo $\mathfrak{p}$ de A , si por $v_{\mathfrak{p}}$ representamos la valoración de K asociada a $\mathfrak{p}$, se tendrá

$$v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(a_i) + n v_{\mathfrak{p}}(b) .$$

Elijamos $\mathfrak{p}$ de modo que

$$v_{\mathfrak{p}}(a_i) = o \quad , \quad \text{para} \quad 1 \leq i \leq m .$$

Bastará escoger un $a \in K^*$ de forma que $v_{\mathfrak{p}}(a)$ no sea múltiplo de n , para llegar a una contradicción.

Lema (1.5).- Sea K un cuerpo global y $\mathfrak{p}$ un divisor primo de K , W una clausura algebraica de $\hat{K}_{\mathfrak{p}}$ y

$$h : \overline{K} \longrightarrow W$$

un K-monomorfismo. Sea $n > 1$ un entero no divisible por la característica de K . Para todo divisor $m > 1$ de n , se verifica

$$h^{-1}(\hat{K}_{\mathfrak{p}}^{*n}) \cap K \not\subset K^{*m} \quad .$$

Demostración :

A partir del monomorfismo h , podemos construir un monomorfismo

$$\frac{K^*}{h^{-1}(\hat{K}_{\mathfrak{p}}^{*n}) \cap K} \longrightarrow \frac{\hat{K}_{\mathfrak{p}}^*}{\hat{K}_{\mathfrak{p}}^{*n}}$$

con lo cual, puesto que $\hat{K}_{\mathfrak{p}}^* / \hat{K}_{\mathfrak{p}}^{*n}$ es un grupo finito ([1], XXI), $h^{-1}(\hat{K}_{\mathfrak{p}}^{*n}) \cap K$ será de índice finito en K^* . Si

$$h^{-1}(\hat{K}_{\mathfrak{p}}^{*n}) \cap K \subset K^{*m} \quad ,$$

de manera natural podríamos construir un epimorfismo

$$\frac{K^*}{h^{-1}(\hat{K}_{\mathfrak{p}}^{*n}) \cap K} \longrightarrow \frac{K^*}{K^{*m}}$$

pero, a la vista de (1.4) , ello sería contradictorio.

Como caso particular, cuando $m = n$, se obtiene que

$$K^{*n} \subsetneq \hat{K}_{\mathfrak{p}}^{*n} \cap K \quad .$$

Concluye así la demostración del teorema (1.3) .

Teorema (1.6).- Sea K un cuerpo global, $\mathfrak{p}$ un divisor primo de K y $q = p^f$ el número de elemen-

tos del cuerpo residual de $\hat{K}_\mathfrak{p}$. Si $n \geq 1$ es un entero no divisible por la característica de K y si las raíces n-ésimas de la unidad están contenidas en $\hat{K}_\mathfrak{p}$, se verifica

$$(K^* K_\mathfrak{p}^{*n} : K_\mathfrak{p}^{*n}) \leq n^2 q^{v_\mathfrak{p}(n)} .$$

Demostración :

Sea $\| \ \|$ el valor absoluto normalizado de $\hat{K}_\mathfrak{p}$. Es sabido que ([1], XXI)

$$(\hat{K}_\mathfrak{p}^* : \hat{K}_\mathfrak{p}^{*n}) = \frac{n}{\|n\|} (E_n : (1))$$

siendo E_n el grupo de las raíces n-ésimas de la unidad contenidas en $\hat{K}_\mathfrak{p}$. Las hipótesis hechas implican que

$$\frac{n}{\|n\|} (E_n : (1)) = n^2 q^{v_\mathfrak{p}(n)} .$$

Sea $h : \overline{K} \longrightarrow W$ el morfismo definido en (1.3). La afirmación del teorema se obtiene al tener en cuenta que

$$\frac{K^* K_\mathfrak{p}^{*n}}{K_\mathfrak{p}^{*n}} \simeq \frac{K^*}{K^* \cap K_\mathfrak{p}^{*n}}$$

y que por (1.3) , h factoriza en un monomorfismo

$$\frac{K^*}{K^* \cap K_\mathfrak{p}^{*n}} \longrightarrow \frac{\hat{K}_\mathfrak{p}^*}{\hat{K}_\mathfrak{p}^{*n}} .$$

<u>Corolario (1.7).-</u> Sea K un cuerpo de números, $\mathfrak{p}$ un divisor primo de K y $n \geq 1$ un entero cumplien-

do las condiciones de (1.6) . Existe una constante $c(n,K,\mathfrak{p})$ tal que, toda forma diagonal

$$a_1 X_1^n + \dots + a_m X_m^n$$

en la que los $a_i \in K^*$ y $m > c(n,K,\mathfrak{p})$ representa cero en $K_{\mathfrak{p}}$.

Demostración :

a) Caso en que n sea impar.

Tomemos $c(n,K,\mathfrak{p}) = n^2 q^{v_{\mathfrak{p}}(n)}$. Por (1.6) deberán existir un par de índices i , j , $i \neq j$, tales que

$$a_i \equiv a_j \mod K_{\mathfrak{p}}^{*n} .$$

Si $a_i = a_j b^n$, para cierto $b \in K_{\mathfrak{p}}^*$,

$$(0, \dots, 1, \overset{i)}{\dots}, -b, \overset{j)}{\dots}, 0)$$

será una representación de cero por la forma considerada.

b) Caso en que n sea par.

Sea d el menor entero positivo tal que

$$-d \in \hat{K}_{\mathfrak{p}}^{*n}$$

(la existencia de d se obtiene a partir del lema de Hensel ([2] , Cap.I, § 5, Teor.3)) . El polinomio $X^n + d$ descompondrá en $\hat{K}_{\mathfrak{p}}$ en producto de factores lineales ;

en consecuencia

$$-d \in K_p^{*n} \quad .$$

Tomemos en este caso

$$c(n,K,p) = (d+1)\, n^2\, q^{v_p(n)} \quad .$$

Si $m > c(n,K,p)$ un cambio de variables definido en K_p nos permitirá transformar la forma dada en la siguiente

$$X_1^n + \ldots + X_{d+1}^n + a'_{d+2}\, X_{d+2}^n + \ldots + a'_m\, X_m^n \quad .$$

Si $e \in K_p^*$ es un elemento tal que

$$e^n = -d$$

bastará tomar

$$X_1 = X_2 = \ldots = X_d = 1 \ ,$$

$$X_{d+1} = e \ ,$$

$$X_{d+2} = \ldots = X_m = o \ ,$$

como representación de cero en K_p por la forma considerada.

Obsérvese que si $n = 2$ o bien si $n \mid q-1$, las raíces n-ésimas de la unidad pertenecen a $\hat{K}_p$, y en este último caso $v_p(n) = o$.

En el § 3 se verá que $c(2,K,\mathfrak{p})$, para $\mathfrak{p} \nmid 2$, puede tomarse igual a 4 .

2. Raíces n-ésimas (continuación)

Proposición (2.1).- Sea K un cuerpo global, $\mathfrak{p}$ un divisor primo de K y $q = p^f$ el número de elementos del cuerpo residual de $\hat{K}_{\mathfrak{p}}$. Sea $t \neq p$ un entero primo. Si $t \nmid q-1$ se verifica

$$K_{\mathfrak{p}}^{*t} \cap L = L^{*t}$$

para todo cuerpo L tal que $K \subset L \subset K_{\mathfrak{p}}$.

Demostración :

Se hará por el absurdo. Supongamos

$$K_{\mathfrak{p}}^{*t} \cap L \supsetneq L^{*t} \quad ;$$

sea $x \in K_{\mathfrak{p}}^{*t} \cap L$ un elemento tal que $x \notin L^{*t}$. Sea $y \in K_{\mathfrak{p}}^{*}$ tal que

$$x = y^t \quad .$$

y definamos $M = K(x)$. Se tendrá que $x \notin M^{*t}$.

Si $\mathfrak{p}_i$, $1 \leq i \leq g$, son los divisores primos de M que dividen a $\mathfrak{p}$, por (II.1.2)

$$\mathfrak{p}_i \in S(M(y)/M) \quad , \quad \text{para} \quad i = 1,\ldots,g \; .$$

Puesto que el polinomio

$$X^t - x$$

es irreducible en M , si $\varepsilon_t \in \bar{K}$ es una raíz primitiva t-ésima de la unidad, $M(y,\varepsilon_t)$ será la clausura galoisiana de $M(y)$ sobre M ; por tanto

$$\mathfrak{P}_i \in S(M(y,\varepsilon_t)/M) \quad , \quad \text{para} \quad i = 1,\ldots,g \ .$$

Al considerar las inclusiones

$$M(y,\varepsilon_t) \supset K(\varepsilon_t) \supset K$$

se tendrá que

$$\mathfrak{p} \in (K(\varepsilon_t)/K)$$

con lo cual, por (1.1), t debería dividir a $q-1$.

Teorema (2.2).- Sea K un cuerpo global, $\mathfrak{p}$ un divisor primo de K y q el número de elementos del cuerpo residual de $\hat{K}_{\mathfrak{p}}$. Si $t \neq p$ es un entero primo tal que $t \nmid q-1$ y n es un entero positivo divisible por t , el índice

$$(K_{\mathfrak{p}}^{*} : K_{\mathfrak{p}}^{*n})$$

es infinito.

Demostración :

Empezaremos considerando el caso en que $n = t$.
De la demostración de (1.3) , o por (2.1), se deduce que

$$K_{\mathfrak{p}}^{*t} \cap K = K^{*t} \ .$$

La inclusión de K en $K_{\mathfrak{p}}$ dará lugar a un monomorfismo

$$K^*/K^{*t} \longrightarrow K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*t}$$

con lo cual, aplicando (1.4), se obtiene el resultado.

En el caso general, si $t' \mid n$, podemos construir de manera natural un epimorfismo

$$K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*n} \longrightarrow K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*t'}$$

con lo que el primero de estos grupos será también no finito.

3. Formas cuadráticas

Teorema (3.1).- Sea K un cuerpo de números, $\mathfrak{p}$ un divisor primo de K no dividiendo a 2. Toda forma cuadrática

$$F(X) = \sum_{i=1}^{m} a_{ii}X_i^2 + 2 \sum_{i<j} a_{ij}X_iX_j$$

en la que los $a_{ij} \in K$ y de rango $n \geq 5$ representa cero en $K_{\mathfrak{p}}$.

Demostración :

Por una transformación lineal no singular de sus variables, la forma F es equivalente a una forma del tipo

$$a_1X_1^2 + \ldots + a_nX_n^2$$

con los $a_i \in K^*$. Sea

$$A = \left\{ \bar{a}_i \mod K_{\mathfrak{p}}^{*2} \; ; \; 1 \leq i \leq n \right\} .$$

De (1.6) se deduce que

$$(K^* K_{\mathfrak{p}}^{*2} : K_{\mathfrak{p}}^{*2}) \leq 4 \quad .$$

Puesto que por hipótesis es $n \geq 5$, existirán elementos $\bar{a}_i$, $\bar{a}_j \in A$, $i \neq j$, tales que

$$\bar{a}_i = \bar{a}_j \quad .$$

Sea $(p) = \mathfrak{p} \cap Z$. En la demostración distinguiremos dos casos según que p sea o no congruente con 1 módulo 4.

a) Caso en que $p \equiv 1 \ (4)$.

Por las reglas de descomposición en un cuerpo cuadrático se tendrá que

$$p \in S(Q(i)/Q)$$

lo cual implica que

$$-1 \in Q_p^{*2} \subset K_{\mathfrak{p}}^{*2} \quad .$$

En este caso

$$\bar{a}_i = \bar{a}_j \Longrightarrow -\bar{a}_i = \bar{a}_j \Longrightarrow \exists\ b \in K_{\mathfrak{p}}^* \text{ tal que } -a_i = a_j b^2,$$

con lo cual

$$(o, \ldots, \underset{i)}{1}, \ldots, \underset{j)}{b}, \ldots, o)$$

será una representación de cero en $K_{\mathfrak{p}}$.

b) Caso en que $p \equiv 3 \ (4)$.

Sea r el número de elementos de A.

Si $r > 2$, existirán elementos $a_i, a_j \in A$, $i \neq j$, y tales que

$$-\bar{a}_i = \bar{a}_j$$

en cuyo caso se procede como en a) .

Si $r \leq 2$, por una transformación no singular, F será equivalente a una forma del tipo

$$X_1^2 + X_2^2 + X_3^2 \dot{+} G$$

en donde G es una forma cuadrática y $\dot{+}$ indica la suma ortogonal. Sea F_p el cuerpo finito de p elementos. Puesto que

$$(F_p^* : F_p^{*2}) = 2 ,$$

se podrá encontrar un entero t tal que $2 \leq t < p$ y

$$\left(\frac{t-1}{p}\right) = +1 , \quad \left(\frac{t}{p}\right) = -1 .$$

La anterior elección implica que

$$p \in S(Q(\sqrt{t-1})/Q) \cap S(Q(\sqrt{-t})/Q) ;$$

en consecuencia,

$$p \in S(K(\sqrt{t-1})/K) \cap S(K(\sqrt{-t})/K)$$

con lo que, a partir de

$$(\sqrt{t-1}, \sqrt{-t}, 1, 0, \ldots, 0)$$

se obtendrá una representación de cero en K_p por F .

Observación (3.2).- En el caso de que K sea un cuerpo de números totalmente imaginario, o un cuerpo global de funciones, teoremas bien conocidos (véase [2] y (III.3.3)) permiten afirmar que toda forma cuadrática de cinco variables

definida en $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ representa cero en dicho cuerpo. En consecuencia (véase [49]) , dos formas cuadráticas F y G definidas en $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ serán isométricas si y sólo si se verifica

$$\text{rang } F = \text{rang } G \ , \quad dF = dG \ , \quad SF \simeq SG \ ,$$

en donde d y S designan el discriminante y el álgebra de Hasse - Minkowski - Witt, respectivamente.

En el caso de que K sea un cuerpo de números con primos reales tenemos la siguiente

Proposición (3.3).- Si K es un cuerpo de números y $\mathfrak{p}_\infty$ un primo real de K , dos formas cuadráticas definidas en $K_{\mathfrak{p}_\infty}$ son isométricas si y sólo si tienen el mismo rango y la misma signatura total (es decir, igual signatura con respecto a todas las ordenaciones de $K_{\mathfrak{p}_\infty}$) .

Demostración :

Por (I.3.4), $K_{\mathfrak{p}_\infty}$ es un cuerpo ordenable. En virtud del principio local-global de Pfister ([31] , Teor.22), la afirmación de la proposición es equivalente a la de que $K_{\mathfrak{p}_\infty}$ sea un cuerpo pitagórico (véase [15]), es decir, que verifique

$$K_{\mathfrak{p}_\infty}^2 + K_{\mathfrak{p}_\infty}^2 = K_{\mathfrak{p}_\infty}^2 \ .$$

Sean $a, b \in K_{\mathfrak{p}_\infty}$ y $c \in \overline{K}$ un elemento tal que $c^2 = a^2+b^2$. Sea $h : K \longrightarrow R$ el monomorfismo asociado a $\mathfrak{p}_\infty$. En virtud de (I.3.4) bastará probar que, para toda extensión de h a un homomorfismo de $\overline{K}$ en $\mathbb{C}$, $h(c) \in R$, lo cual es inmediato.

Capítulo V

PRINCIPIO DE HASSE CON CUERPOS TOTALMENTE p-ADICOS

Introducción.

El más célebre de los principios local - global es sin duda el principio de Hasse para formas cuadráticas :

Dada una forma cuadrática F cuyos coeficientes pertenecen a un cuerpo global K, F representa cero en K si y sólo si F representa cero en todos los completados $\hat{K}_p$.

Si se reemplaza F por un polinomio de una variable, el principio anterior deja de verificarse (véase [21]). Contraejemplos en formas de grado par fueron dados por Artin [24] y por Reichardt [33], y en formas de grado impar por Selmer [36], Swinnerton - Dyer [44], Mordell [27], Cassels - Guy [lo], y recientemente, por Fujiwara [17].

En este capítulo se formula un principio semejante al de Hasse, pero en el que los cuerpos $\hat{K}_p$ son reemplazados por los cuerpos $K_{p_1,\ldots,p_r}$.

Esta nueva formulación, sugerida por un resultado obtenido por F. Tomás (véase [45], Teor.1), permite tratar con éxito el caso de polinomios de una variable y de formas binarias. El contraejemplo de Artin para formas de grado par, deja de ser un contraejemplo cuando se consideran los cuerpos anteriores y permite dar una familia de formas en las que es válido el nuevo principio. Tal ocurre también con otros contraejemplos clásicos fabricados a partir de

formas descomponibles.

En los casos estudiados se pone de manifiesto la necesidad de considerar no sólo los cuerpos $K_\mathfrak{p}$, sino los cuerpos $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ formados a partir de intersecciones finitas de aquellos (tal necesidad aparece ya en el estudio de polinomios de una variable) , así como la de considerar todos los primos de K , incluidos los infinitos.

Finalmente destaquemos que otras situaciones de validez del principio de Hasse, como son los ejemplos de Hasse [21], Selmer [37], Châtelet [11] y Skolem [43] así como el principio local - global en álgebras simples [1], son válidas " a fortiori " al reemplazar los cuerpos $\mathfrak{p}$-ádicos por los cuerpos totalmente $\mathfrak{p}$-ádicos.

1. Una aplicación de la función zeta de Dedekind

En este apartado se indica por K un cuerpo global, por P el conjunto de sus divisores primos y por P_∞ el de sus primos infinitos. Para cada $\mathfrak{p} \in P$ representamos por $q_\mathfrak{p}$ el número de elementos del cuerpo residual de $\hat{K}_\mathfrak{p}$.

Dado $\sigma \in R$, el producto de Euler

$$\zeta_K(\sigma) = \prod_{\mathfrak{p} \in P} \frac{1}{1 - q_\mathfrak{p}^{-\sigma}}$$

es convergente para $\sigma > 1$ y verifica , $\lim_{\sigma \to +\infty} \zeta_K(\sigma) = 1$ ([47] , Cap.VII, Prop.1).

A partir de la convergencia del producto de Euler se obtiene que, para todo $s \in \mathbb{C}$ tal que $\mathrm{Re}(s) > 1$, el

producto

$$\zeta_K(s) = \prod_{\mathfrak{p} \in P} \frac{1}{1 - q_{\mathfrak{p}}^{-s}}$$

es absolutamente convergente. ζ_K es por tanto una función holomorfa y sin ceros en $Re(s) > 1$. Dicha función se prolonga analíticamente a una función meromorfa en el plano con un único polo en $s = 1$ ([47], Cap.VII, § 6). Se obtiene así la función zeta de Dedekind del cuerpo K .

Se recuerdan a continuación ciertas propiedades, necesarias para la demostración del lema (1.4) que se da a continuación.

(1.1) Sea K_o un cuerpo global contenido en K , $M \subset P$ un subconjunto tal que, para casi todo $\mathfrak{p} \in M$ (es decir, para todo $\mathfrak{p} \in M$ salvo a lo sumo en un número finito de casos), se verifique

$$f_{\mathfrak{p}}(K/K_o) > 1 \ .$$

Entonces, para $Re(s) > 1/2$, el producto

$$\prod_{\mathfrak{p} \in M} \frac{1}{1 - q_{\mathfrak{p}}^{-s}}$$

es absolutamente convergente; define en consecuencia una función holomorfa en s y sin ceros.

(1.2) Si N es un conjunto finito de primos de K tal que $P_\infty \subset N$, el producto

$$p(K,N,s) = \prod_{\mathfrak{p} \notin N} \frac{1}{1 - q_{\mathfrak{p}}^{-s}}$$

es absolutamente convergente para $\mathrm{Re}(s) > 1$.

Las propiedades anteriores son consecuencia inmediata de la convergencia del producto de Euler. A su vez, la ecuación funcional ([47] , Cap. VII , § 5) permite obtener que existe el siguiente límite

$$\lim_{s \longrightarrow 1} (s-1)\, p(K,N,s)$$

y es finito y mayor que cero.

(1.3) Sea $V \subset P$ un subconjunto tal que, para casi todo $p \in P - V$

$$f\,(K/K_o) > 1 .$$

De (1.1) y de (1.2) se deduce entonces que el producto

$$q(K,V,s) = \prod_{p \in V} \frac{1}{1 - q_p^{-s}}$$

es absolutamente convergente para $\mathrm{Re}(s) > 1$ y que

$$\lim_{s \longrightarrow 1} (s-1)\, q(K,V,s)$$

es finito y mayor que cero. Para verlo basta hacer $N = P_\infty$, $M = P - V$ y formar la descomposición

$$p(K,N,s) = q(K,V,s) \prod_{p \in M} (1 - q_p^{-s})^{-1}$$

<u>Lema (1.4).-</u> Sea K un cuerpo global y S un conjun-

to finito de primos de K , se verifica

$$\bigcap_{\mathfrak{p} \notin S} K_{\mathfrak{p}} = K \ .$$

Demostración :

La demostración es en esencia la de [47], Cap.VII, § 5, Cor.4 . Sea L una extensión finita de K tal que

$$K \subset L \subset \bigcap_{\mathfrak{p} \notin S} K_{\mathfrak{p}} \ .$$

Sea V el conjunto de los divisores primos de K que descomponen completamente en L . Por (1.2) , el producto

$$q(K,V,s) = \prod_{\mathfrak{p} \in V} \frac{1}{1 - q_{\mathfrak{p}}^{-s}}$$

es absolutamente convergente para $Re(s) > 1$ y $(s-1)\, q(K,V,s)$ tiende a un límite finito y mayor que cero cuando s tiende a uno.

Sea W el conjunto de los divisores primos de L cuya restricción a K pertenece a V . De (1.3) se deduce que el producto

$$q(L,W,s) = \prod_{\mathfrak{P} \in W} \frac{1}{1 - q_{\mathfrak{P}}^{-s}}$$

es absolutamente convergente para $Re(s) > 1$ y que

$$\lim_{s \longrightarrow 1} (s-1)\, q(L,W,s)$$

es finito y mayor que cero.

La elección de L implica que, si $\mathfrak{p} \in W$ y la restricción de $\mathfrak{p}$ a K es $\mathfrak{p}$,

$$q_{\mathfrak{p}} = q_{\mathfrak{p}}$$

y

$$q(L,W,s) = q(K,V,s)^n$$

siendo $n = [L : K]$. De las consideraciones anteriores se deduce que $n = 1$.

Observación (1.5).- El lema anterior, necesario para la demostración del teorema (2.1) que se da a continuación, hubiera podido deducirse fácilmente a partir de [47], Cap.XIII, § 12, Teor.12 ; es decir, de la versión del teorema de Tchebotarev válida en cuerpos globales. Se ha preferido, no obstante, su deducción a partir del uso exclusivo de la función zeta, por cuanto que ello representa una "economía de recursos" .

2. Polinomios de una variable y formas binarias

Teorema (2.1).- Sea K un cuerpo global y f(X) un polinomio de una variable cuyos coeficientes pertenecen a K . Sea S un conjunto finito de primos de K y consideremos ordenado el conjunto (numerable) de los primos de K no pertenecientes a S . Se verifica :

a) La ecuación $f(X) = o$ es resoluble en K si y sólo si lo es en todos los cuerpos totalmente $\mathfrak{p}$-ádicos

$K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$, formados a partir de los primos $\mathfrak{p}_i$ de K no pertenecientes a S .

b) El polinomio $f(X)$ es reducible en K si y sólo si es reducible en todos los cuerpos $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ anteriormente considerados.

Demostración :

Representemos por C_r el conjunto de ceros de f en $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$. Puesto que

$$K_{\mathfrak{p}_1} \supset K_{\mathfrak{p}_1,\mathfrak{p}_2} \supset \cdots \supset K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r} \supset \cdots$$

se tendrá que

$$C_1 \supset C_2 \supset \cdots \supset C_r \supset \cdots .$$

Si suponemos que $C_r \neq \emptyset$, para todo $r \geq 1$, existirá un elemento $x \in \overline{K}$ tal que

$$x \in \bigcap_{r \geq 1} C_r .$$

Puesto que $x \in \bigcap_{\mathfrak{p} \notin S} K_{\mathfrak{p}}$, por (1.4) , $x \in K$.

b) Sea D_r el conjunto de los divisores propios de f pertenecientes a $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}[X]$. Se tendrá que

$$D_1 \supset D_2 \supset \cdots \supset D_r \supset \cdots .$$

Si $D_r \neq \emptyset$, para cada $r \geq 1$, por ser éstos también conjuntos finitos, existirá un elemento

$$h(X) \in \bigcap_{r \geq 1} D_r$$

que será, por (1.4) , un divisor propio de f en $K[X]$.

Es posible que un polinomio $f \in K[X]$ tenga solución en todos los cuerpos K_p , asociados a un sólo primo, sin que la tenga en K . Lo mismo puede decirse del carácter reducible de f . Ello se pone de manifiesto en los siguientes ejemplos.

Ejemplo (2.2).- Dados dos enteros primos impares p , q tales que

$$\left(\frac{p}{q}\right) = +1 \quad y \quad p \equiv 1 \ (8) \quad ,$$

el polinomio

$$f(X) = (X^2 - p)(X^2 - q)(X^2 - pq)$$

tiene solución en todos los cuerpos Q_t , al recorrer t todos los enteros primos, pero no tiene solución en Q .

Demostración :

Por ser f un producto de factores de segundo grado, para probar que es resoluble en Q_t , bastará ver que tiene una solución en cada completado $\hat{Q}_t$.

Sea $x \in \hat{Q}_t^*$, $x = t^n u$, en donde u es un unitario de $\hat{Z}_t$. Por ([2], Cap.I, § 6, Teor.1 y 2) se tendrá :

Si $t \neq 2$, $x \in \hat{Q}_t^{*2} \iff$ n es par y la imagen de u en F_t^* es un cuadrado .

Si $t = 2$, $x \in \hat{Q}_2^{*2} \iff$ n es par y $u \equiv 1\ (8)$.

De $\left(\frac{p}{t}\right)\left(\frac{q}{t}\right)\left(\frac{pq}{t}\right) = +1$, para todo primo $t \neq p, q$, se deduce por tanto que, para $t \neq 2, p, q$, f tiene un cero en Q_t .

Puesto que $p \equiv 1\ (4)$, la hipótesis hecha y la ley de reciprocidad cuadrática ([4o], Cap.I, Teor.6) garantizan que

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = +1 ,$$

con lo cual f representará cero en Q_p y en Q_q .

El hecho de que f represente cero en Q_2 se deduce de que $p \equiv 1\ (8)$.

Puesto que $X^2 - p$ es irreducible en Q_p , $X^2 - q$ lo es en Q_q y $X^2 - pq$ lo es en Q_p y en Q_q , se tiene que f no representa cero en $Q_{p,q}$.

El ejemplo más sencillo de primos p y q satisfaciendo las hipótesis del enunciado lo constituyen los primos $p = 17$, $q = 13$.

(Polinomios como el anterior fueron considerados por E. Artin para poner un contraejemplo a una afirmación de U. Wegner, véase [21]) .

Ejemplo (2.3).- Sean p, q dos enteros primos verificando las condiciones del ejemplo anterior. Sea $x = \sqrt{p} + \sqrt{q}$ y f el polinomio minimal de x sobre $\mathbf{Q}$. Para todo entero primo t , f es reducible en Q_t .

Demostración :

Por ser $Q(x)$ una extensión abeliana de Q y por (I.4.1) tendremos

$$\left[Q_t(x) : Q_t \right] = n_t(Q(x)/Q) .$$

Bastará por tanto probar que, para cada t, es $n_t < 4$.

Los primos que ramifican en $Q(x)$ son p, q y posiblemente el 2 (si $q \equiv 2$ ó 3 (4)). Ya que

$$G(Q(x)/Q) \simeq Z/(2) \times Z/(2)$$

y los grupos de descomposición en un primo no ramificado son cíclicos, tendremos que

$$n_t(Q(x)/Q) < 4 \qquad \text{si } t \neq p, q, 2 .$$

Puesto que $2 \in S(Q(\sqrt{p})/Q)$, $n_2(Q(x)/Q) \leq 2$.

Si $t = p$, de $\left(\frac{q}{p}\right) = \pm 1$, se sigue que $p \in S(Q(\sqrt{q})/Q)$, con lo cual $n_p(Q(x)/Q) = 2$. Si $t = q$, basta intercambiar p y q en el razonamiento anterior para obtener que $n_q(Q(x)/Q) = 2$.

Del teorema (2.1) se deduce a su vez el siguiente

<u>Corolario (2.4).-</u> Sea K un cuerpo global y $F(X,Y)$ una forma a coeficientes en K. $F(X,Y)$ representa cero en K si y sólo si F representa cero en todos los cuerpos $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$, elegidos como en (2.1).

Demostración : No es restrictivo suponer que Y no divide a F. Sea $f(X) = F(X,1)$. Basta tener en cuenta que $F(X,Y)$ representa cero en K si y sólo si $f(X)$ tiene un cero en K y aplicar (2.1).

La afirmación de (2.4) formulada en el caso p-ádico y para formas irreducibles era conocida a través del resultado de Hasse para polinomios irreducibles ([21] y [17]).

3. Sumas de cuadrados

Se ha visto en el apartado anterior que una forma binaria representa cero en un cuerpo global K si y sólo si lo hace en todos los cuerpos $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$, pudiendo excluirse un conjunto finito S de primos de K. Si K es un cuerpo de números, puede tomarse en particular $S = P_\infty$. Cuando el número de variables se aumenta, es necesario tener en cuenta los primos infinitos de K. Ello se pone de manifiesto con ejemplos que damos en este apartado.

Proposición (3.1).- Sea K un cuerpo de números. Para todo entero $n \geq 5$ y para toda elección finita de divisores primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ de K, la forma

$$X_1^2 + \ldots + X_n^2$$

representa cero en $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$.

Demostración :

Sea $(p_i) = \mathfrak{p}_i \cap \mathbb{Z}$, para $i = 1, \ldots, r$. Por (II.1.2) será suficiente probar que la forma

$$X_1^2 + \ldots + X_n^2$$

representa cero en $\mathbb{Q}_{p_1,\ldots,p_r}$.

Sin restricción podemos suponer que $p_1 = 2$. Sean $p_2, \ldots, p_s$ los primos anteriormente obtenidos congruentes con 1 módulo 4 y $p_{s+1}, \ldots, p_r$ los congruentes con 3 módulo 4 (sin restricción también, podemos suponer que ambos subconjuntos son no vacíos) . Sea

$$a = \prod_{i=2}^{s} p_i \quad , \quad b = \prod_{i=s+1}^{r} p_i$$

y sea

$$c = -a^2 + b^2 + 7(ab)^2 .$$

Aumentando si es preciso el número de enteros primos congruentes con 3 módulo 4 , podemos suponer que es $c > 0$.

Se verifican las siguientes relaciones :

$$\left(\frac{c}{p_i}\right) = +1 \qquad \text{para } i = 2,\ldots,s$$

$$\left(\frac{c}{p_j}\right) = \left(\frac{-a^2}{p_j}\right) = \left(\frac{-1}{p_j}\right) = -1 \quad \text{para } j = s+1,\ldots,r$$

$$a^2 \equiv b^2 \equiv 1 \ (8) \ ,$$

las cuales implican

$$\left(\frac{-c}{p_i}\right) = +1 \qquad \text{si} \quad p_i \equiv 1 \ (4)$$

$$\left(\frac{-c}{p_j}\right) = +1 \qquad \text{si} \quad p_j \equiv 3 \ (4)$$

$$c \equiv -1 \ (8) \ .$$

Las condiciones anteriores permiten asegurar que

$$\sqrt{-c} \in Q_{2,p_2,\ldots,p_r} \ .$$

Ya que c es un entero mayor que cero, por el teorema de Lagrange ([4o], Cap.IV, Apéndice, Cor.1) podemos encontrar cuatro enteros a_i tales que

$$c = a_1^2 + a_2^2 + a_3^2 + a_4^2 \ .$$

En consecuencia

$$(\sqrt{-c}, a_1, a_2, a_3, a_4, o, \ldots, o)$$

será una representación de cero de la forma considerada.

(Para formas diagonales y utilizando únicamente divisores primos, no cabe por tanto esperar un principio de Hasse. Es evidente que la forma anterior no representa cero en Q) .

Corolario (3.2).- Dado un cuerpo de números K y un

conjunto finito $\{\mathfrak{p}_i\}_{1 \leq i \leq r}$ de primos de K, el cuerpo $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ es ordenable si y sólo si algún $\mathfrak{p}_i$ es un primo infinito real.

Demostración :

Por el teorema de Artin-Schreier ([4], Cap.VI, § 2, Cor.1 al Teor.1), un cuerpo K es ordenable si y sólo si una relación de la forma

$$\sum_{i=1}^{n} x_i^2 = 0 \quad , \quad x_i \in K$$

implica que $x_i = 0$, para $i = 1, \ldots, n$. En consecuencia, por (3.1) si todos los $\mathfrak{p}_i$ son divisores primos de K, $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ no es ordenable.

Si algún $\mathfrak{p}_i$ es real, basta tener en cuenta que, por (I.3.4), $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ será isomorfo a un subcuerpo de R.

Observación (3.3).- El hecho de que para cierto $n > 1$, la forma $D_n = \sum_{i=1}^{n} X_i^2$ represente cero en todos los cuerpos $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$ obtenidos a partir de un cuerpo de números K, es equivalente a que K sea un cuerpo totalmente imaginario y en consecuencia, a que la forma anterior, para un $n = n(K)$ represente cero en K. (Esto último es debido a que, dado un cuerpo de números K, las estructuras del mismo como cuerpo ordenable están en correspondencia biyectiva con sus primos infinitos reales ([4], Cap.VI, § 2, ejer.28 ; o bien [34], Cap.IX, Teor.1o)).

4. Formas del tipo $(X_1^2 + \ldots + X_n^2)^m - a(Y_1^2 + \ldots + Y_n^2)^m$

La forma siguiente

$$(X_1^2 + \ldots + X_n^2)^2 - 2(Y_1^2 + \ldots + Y_n^2)^2 \quad \text{para} \quad n \geq 5 \ ,$$

fué indicada por Artin [24] , como contraejemplo de principio de Hasse. Dicha forma representa cero en R , en todos los cuerpos $\hat{Q}_p$ y no representa cero en Q .

En el caso totalmente p-ádico tenemos la siguiente

Proposición (4.1).- Sea K un cuerpo de números ordenable y a un elemento de K no nulo .

Dadas las formas

$$F_n = (X_1^2 + \ldots + X_n^2)^m - a(Y_1^2 + \ldots + Y_n^2)^m \ ,$$

en las que se supone que m es impar si K posee más de un primo real, las siguientes afirmaciones son equivalentes :

a) Para toda elección finita de primos de K , existe un $n \geq 1$ tal que F_n representa cero en $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$.

b) $a \in K^{*m}$ y es un elemento de K totalmente positivo .

c) Existe un entero $n = n(a,K)$, $n \geq 1$, tal que F_n representa cero en K .

Si $K = Q$, n se puede tomar igual a 4 para todo a verificando las condiciones de b) .

(Obsérvese que si K no es ordenable, existe un $n = n(K)$ tal que F_n representa siempre cero en K).

Demostración :

Supongamos ordenado el conjunto de primos de K de forma que $\mathfrak{p}_1 = \mathfrak{p}_\infty$ sea un primo infinito real. Dada una representación de F_n en $K_{\mathfrak{p}_1,\dots,\mathfrak{p}_r}$ con $n \geq 1$

$$(x_1^{(r)}, \dots, x_n^{(r)} ; y_1^{(r)}, \dots, y_n^{(r)}) ,$$

de (3.2) se deduce que

$$\sum_{i=1}^{n} (y_i^{(r)})^2 \neq 0 \qquad (1)$$

y en consecuencia

$$a \in K^{*m}_{\mathfrak{p}_1,\dots,\mathfrak{p}_r} .$$

Bajo las condiciones de a) , el polinomio $X^m - a$ representará cero en todos los cuerpos $K_{\mathfrak{p}_1,\dots,\mathfrak{p}_r}$; por (2.1) se tendrá por tanto que

$$a \in K^{*m} .$$

Puesto que todo producto y todo cociente de sumas de cuadrados es a su vez una suma de cuadrados, de (1) se deduce también que

$$a \in \sum K^2_{\mathfrak{p}_1,\dots,\mathfrak{p}_r}$$

(indicando por $\sum K^2$ los elementos de K que se expresan como suma de cuadrados). En consecuencia, en toda ordenación de cuerpo de $K_{\mathfrak{p}_1,\ldots,\mathfrak{p}_r}$, a debe ser un elemento positivo. Ya que toda ordenación de K como cuerpo se puede obtener por restricción de una ordenación de $K_{\mathfrak{p}_\infty}$, para un primo real de K convenientemente elegido ([34], Cap.IX, Teor.1o), las consideraciones anteriores implican que a sea un elemento de K totalmente positivo. En consecuencia a) $\Longrightarrow$ b) .

Supongamos cumplidas las condiciones de b) . Sea $b \in K$ un elemento tal que

$$a = b^m$$

y $\sigma : K \longrightarrow R$ un monomorfismo. De $\sigma a = (\sigma b)^m$ se sigue que si $\sigma a > o$ y m es impar ,

$$\sigma b > o .$$

Si σ es el único monomorfismo de K en R , se puede tomar b de modo que $\sigma b > o$, sin necesidad de hacer hipótesis alguna sobre m .

Por el teorema de Landau ([34], Cap.IX, t)) , b será un elemento de K totalmente positivo y en consecuencia

$$b \in \sum K^2 .$$

Si $b = \sum_{i=1}^{n} x_i^2$ es una representación de b como suma de cuadrados en K

$$(x_1 , \ldots , x_n ; 1 , o , \ldots , o)$$

será una representación de cero por F_n . Ello prueba que b) $\Longrightarrow$ c) .

La implicación c) $\Longrightarrow$ a) es inmediata.

Si $K = Q$, el hecho de que $n = 4$ resulta del teorema de Lagrange.

5. Otros ejemplos

Es conocido el siguiente contraejemplo del principio de Hasse clásico : Dados q , t , q' , t' enteros primos distintos tales que

$$\left(\frac{t}{q}\right) = -1 \quad , \quad \left(\frac{t'}{q'}\right) = -1 \ ,$$

si la forma

$$X^2 + q\,Y^2 - tZ^2$$

representa cero en $\hat{Q}_2$, la forma

$$(X^2 + qY^2 - tZ^2)\,(X^2 + q'Y^2 - t'Z^2)$$

representa cero en todos los cuerpos $\hat{Q}_p$ y en R , pero no representa cero en Q .

Sin embargo en nuestro caso no es un contraejemplo como prueba la siguiente

Proposición (5.1).- La forma

$$(X^2 + qY^2 - tZ^2)\,(X^2 + q'Y^2 - t'Z^2)$$

construida bajo las condiciones anteriores , no representa cero en $Q_{q,q'}$.

Demostración :

Sea $A = X^2 + qY^2 - tZ^2$ y $A' = X^2 + q'Y^2 - t'Z^2$. Ya que $\left(\frac{t}{q}\right) = -1$, se sigue que A no representa ceró en $\hat{Q}_q$. Análogamente, A' no puede representar cero en $\hat{Q}_{q'}$.

Sea (x,y,z) una terna de elementos de $Q_{q,q'}$ no todos nulos . Por (I.2.4) podemos construir monomorfismos

$$\sigma : Q_{q,q'} \longrightarrow \hat{Q}_q$$

$$\sigma' : Q_{q,q'} \longrightarrow \hat{Q}_{q'} \quad .$$

El primero de ellos obliga a que

$$A(x,y,z) \neq o$$

y el segundo, a que

$$A'(x,y,z) \neq o \ ,$$

por lo que $A\,A'$ no representa cero en $Q_{q,q'}$.

Está claro que todos los contraejemplos de principio de Hasse, construidos de manera análoga a la anterior, con formas descomponibles, no serán contraejemplos al considerarse los cuerpos totalmente p-ádicos.

Bibliografía citada

[1] Artin,E.,Tate,J.: Class Field Theory. Benjamin, 1967.

[2] Borevitch,Z.I.,Shafarevitch,I.R.: Théorie des Nombres. Gauthier-Villars, 1967.

[3] Bourbaki,N.: Algèbre, Ch.IV-V. Hermann, 1967.

[4] Bourbaki,N.: Algèbre, Ch.VI-VII. Hermann, 1964.

[5] Bourbaki,N.: Algèbre Commutative, Ch.V-VI. Hermann, 1964.

[6] Bourbaki,N.: Algèbre Commutative, Ch.VII. Hermann,1965.

[7] Brauer,R.: A note on systems of homogeneous algebraic equations. Bull.Amer.Math.Soc.,51,1945, p.749-755.

[8] Capelli,A.: Sulla riductibilità della funzione $x^n - A$ in un campo qualunque de rationalità. Math.Ann., 54, 1901, p.602-663.

[9] Cassels,J.W.S.,Frölich,A.: Algebraic Number Theory. Acad.Press., 1967.

[10] Cassels,J.W.S.,Guy,M.J.T.: On the Hasse principle for cubic surfaces. Mathematika,13,1966, p.111-120.

[11] Châtelet,F.: Variations sur un thème de Poincaré. Ann. Sci.Ecole Norm.Sup.,61, 1944, p.249-300.

[12] Cougnard,J.: Construction des extensions galoisiennes non abeliennes d'ordre p q (p et q premiers) du corps des rationnels. Séminaire de Théorie des Nombres. Université de Bordeaux I, 1971-1972, exp. 10 bis.

[13] Deuring,M.: Algebren. Ergeb.der Math.,nº41. Springer, 1968.

[14] Deuring,M.: Lectures on the Theory of Algebraic Functions of One Variable. Lect.Notes in Math.,nº 314. Springer, 1973.

[15] Elman,R.,Lam,T.Y.: Classification Theorems for Quadratic Forms over Fields. Comment.Math.Helv. 49,1974,p.373-381.

[16] Endler,O.: Valuation Theory. Springer, 1972.

[17] Fujiwara,M.: Hasse Principle in algebraic equations. Acta Arith.,XXII,1973, p.267-276.

[18] Golod,E.S.,Shafarevitch,I.R.: On class field towers. Amer.Math.Soc.Transl.,Ser.2,48,1965, p.91-1o2.

[19] Greenberg,M.J.: Lectures on Forms in Many Variables. Benjamin, 1969.

[2o] Hasse,H.: Zwei Existenztheoreme über algebraische Zahlkörper. Math.Ann.,95,1926, p.229-238.

[21] Hasse,H.: Zwei Bemerkungen zu der Arbeit "Zur Arithmetik der Polynome" von U.Wegner in den Mathematischen Annalen,Bd.1o5,S.628 - 631. Math.Ann.,1o6, 1939, p.455 - 456.

[22] Hochschild,G.,Serre,J.P.: Cohomology of group extensions. Trans.Amer.Math.Soc.,74,1953, p.11o - 134.

[23] Krull,W.: Über einen Existenzsatz der Bewertungstheorie. Abh.Math.Sem.Hamburg,23,1959,p.29 - 35.

[24] Lang,S,: Some theorems and conjectures in diophantine equations. Bull.Amer.Math,Soc.,66,196o,p.24o - 249.

[25] Lang,S.: Algebra. Addison - Wesley, 1965.

[26] Lang.S.: Algebraic Number Theory. Addison-Wesley.1970.

[27] Mordell,L.J.: On the conjecture for the rational points on a cubic surface. Journal London Math.Soc.,40, 1965, p.149-158.

[28] Neukirch,J.: Über eine algebraische Kennzeichnung der Henselkörper. J.Reine Angew.Math.,231,1968,p. 75-81.

[29] Neukirch,J.: Kennzeichnunug der p-adischen und der endlichen algebraischen Zahlkörper. Invent.Math.,6, 1969, p. 296-314.

[30] Peck,L.G.: Diophantine equations in algebraic number fields. Amer.J.of Math.,71,1949, p.387-402.

[31] Pfister,A.: Quadratische Formen in beliebigen Körpern. Invent.Math.,1,1966, p. 116-132.

[32] Poitou,G.: Cohomologie galoisienne des modules finis. Dunod, 1967.

[33] Reichardt,H.: Einige im Kleinen überal lösbare, im grossen unlösbare diophantische Gleichungen. J.Reine Angew.Math.,184,1942, p.12-18.

[34] Ribenboim,P.: L'Arithmétique des corps. Hermann, 1972.

[35] Schinzel,A.: Les extensions pures et les résidus des puissances. Journées Arithmétiques. Bordeaux, 1974, (por aparecer).

[36] Selmer,E.S.: The diophantine equation $a x^3 + b y^3 + c z^3 = 0$. Acta Math.,85, 1951, p. 203-362.

[37] Selmer,E.S.: Sufficient congruence conditions for the existence of rational points on certain cubic surfaces. Math.Scand., 1, 1953, p. 113-119.

[38] Serre,J.P.: Cohomologie Galoisienne. Lect.Notes in Math.,nº 5 .Springer,1965.

[39] Serre,J.P.: Corps locaux. Hermann, 1968.

[4o] Serre,J.P.: Cours d'arithmétique. Press.Univ. de France, 197o.

[41] Shafarevitch,I.R.: Construction of fields of algebraic numbers with given solvable Galois group. Amer.Math. Soc.Transl.,Ser.2,4,196o, p.185 - 237.

[42] Shatz,S.S.: Profinite groups, arithmetic, and geometry. Ann.of Math.Studies. Princeton, 1972.

[43] Skolem,T.: Einige Bemerkungen über die Auffindung der rationalen Punkte auf gewissen algebraischen Gebilden. Math.Z.,63,1955, p.295 - 312.

[44] Swinnerton - Dyer,H.P.F.: Two special cubic surfaces. Mathematika,9,1962, p.54 - 56.

[45] Tomás,F.: Sobre los normalizados de los grupos de descomposición. Anales del Instituto de Matemáticas, U.N.A.M.,1973 (por aparecer).

[46] Tomás,F.: Un análogo de suma directa para sistemas de subgrupos normales. Anales del Instituto de Matemáticas, U.N.A.M., 1973 (por aparecer).

[47] Weil,A.: Basic Number Theory. Springer, 1967.

[48] Weiss,E.: Cohomology of groups. Acad.Press, 1969.

[49] Witt,E.: Theorie der quadratischen Formen in beliebigen Körpern.J.Reine Angew.Math.,176,1936, p.31 - 44.

[5o] Zariski,O.,Samuel,P.: Commutative Algebra, vol.I. Van Nostrand, 1958.