NOTAS DE MATEMATICA

Nº 139

CARACTERIZACIONES ARITMETICAS DE ALGUNOS ANILLOS ENTEROS ALGEBRAICOS

POR

FRANCISCO RIVERO

UNIVERSIDAD DE LOS ANDES
FACULTAD DE CIENCIAS
DEPARTAMENTO DE MATEMATICA
MERIDA - VENEZUELA
1994

Caracterizaciones aritméticas de algunos anillos de enteros algebraicos

Francisco Rivero*
Departamento de Matemática, Universidad de Los Andes
Mérida, **Venezuela**

*Financiamiento CDCHT Universidad de Los Andes - Proyecto C-557-92

Contenido

Abstract

Se conocen caracterizaciones aritméticas para ciertos anillos de enteros algebraicos con grupo de clases de ideales pequeños. Se pueden extender estos resultados, usando el concepto de la Constante de Davenport.

1 Introducción

El anillo de enteros algebraicos de un cuerpo de números, es el ejemplo más conocido de un Dominio de Dedekind. Este anillo R no es un dominio de Factorización Unica en general. Si G es el grupo de clases de ideales de R, entonces R es es DFU si y sólo si G es el grupo trivial.
En 1960 L.Carlitz [1] dió una caracterización de los anillos de enteros de enteros algebraicos con grupo de clases G, tal que el orden de G es menor o igual dos. Un anillo A se denomina **Anillo de factorización media** si para todo elemento x de A, el cual posee dos factorizaciones distintas como producto de irreducibles

$$x = a_1 a_2 \dots a_r = b_1 b_2 \dots b_t$$

se tiene entonces, $r = t$.
Carlitz probó que R es un dominio de Factorización media si y sólo si el orden de G es menor o igual a dos.
Más tarde W.Narkiewicz [14], propuso estudiar las propiedades aritméticas de aquellos anillos de enteros con número de clases de ideales distintos de 1 y 2.
A partir de 1980 comienzan a aparecer algunos resultados importantes en esta dirección: Czogala [3], Di Franco y F. Pace [6], Kaczorowski [9], Krause [10], J.L.Stefan [20], y otros.
En cada uno de estos artículos se dan propiedades aritméticas de R las cuales dependen del grupo G. Por ejemplo, si si en el anillo R, se tienen dos factorizaciones distintas para un mismo elemento

$$a_1 a_2 \dots a_r = b_1 b_2 \dots b_s$$

donde los a_i , b_i son elmentos irreducibles, entonces el máximo de los cocientes r/s se denomina la **Elasticidad del anillo**. Este concepto está relacionado con las propiedades del grupo de clases G.
Si $g_1, g_2, \dots, g_s$ es una sucesión de elementos del grupo G con la propiedad $g_1 g_2 \dots g_s = 1$, y nigún subproducto de ellos sea la identidad, entonces el máximo de tales s, se llama la **Constante de Davenport** del grupo G, la cual se denota por $D(G)$.
Veremos entonces que la constante de Davenport esta intimamente relacionada con la elasticidad del anillo. Por otro lado existe una relación entre el

número de clases h, del anillo R y la constante de Davenport del grupo de clases G.

En este trabajo se estudian las conexiones etre algunas de estas propiedades, siendo el concepto unificador de todas ellas la constante de Davenport de G. Hasta el presente se han caracterizado aquellos anillos con $D(G) \leq 4$. En la parte final daremos una caracterización de anillos de enteros algebraicos con $D(G) = 5$.

Deseo expresar mi mas profundo agradecimiento al Dr. Pedro Berriztbeitia de la Universidad Simón Bolívar, por su valiosa colaboración en el desarrollo de este trabajo. También a los profesores Wilman Brito y Jesus Rivero por su dedicación y empeño demostrados en la difícil tarea de iniciarme en el latex. Gracias también al Laboratorio de Computación del Departamento de Matemáticas por permitirme procesar este trabajo.

Este proyecto fue financiado por el Consejo de Desarrollo Científico y Humanístico de la Universidad de Los Andes, Proyecto C-557-92.

2 Anillo de enteros algebraicos

En esta sección daremos una serie de nociones básicas de la teoría algebraica de números, como lo son el Anillo de Enteros Algebraicos y los Dominios de Dedekind. Para un estudio detallado de estos tópicos se recomienda seguir [17].

Definición 2.1 *Sea F un cuerpo y K una extensión de F. Un elemento $\alpha \in K$ se dice* **Algebraico sobre sobre F** *si α satisface un polinomio*

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = 0$$

donde $a_i \in F$.

Si $p(x)$ es el polinomio de grado mínimo, el cual satisface $p(\alpha) = 0$, entonces diremos que α es **Algebraico de grado** n

Definición 2.2 *Sea K una extensión del cuerpo F. Si todos los elementos de K son algebraicos sobre F entonces K se dice que es una* **Extensión Algebraica de F.**

Por ejemplo $Q(\sqrt{2})$ es una extensión algebraica de Q , cuyos elementos son de la forma $a + b\sqrt{2}$, con a y b números racionales.

Observación 1 *Si K es una extensión algebraica de F entonces se puede probar que K es una extensión finita de F y además finitamente generada. Además, si el grado de K sobre F es n, $[K : F] = n$, entonces todos los elementos de K son algebraicos sobre F de grado $\leq n$.*

Definición 2.3 *Un* **Cuerpo de Números K** *es cualquier extensión finita (y por tanto algebraica) de Q.*

Definición 2.4 *Sea K un cuerpo de números y $\alpha \in K$. Diremos que α es un* **Entero Algebraico** *si satisface un polinomio mónico $p(x) = 0$ con coeficientes en Z.*

Observación. Se demuestra que el conjunto de los enteros algebraicos de un cuerpo K es un anillo, el cual se denota por I_K. Este anillo I_K se llama **Anillo de Enteros Algebraicos del cuerpo** F. El concepto de entero algebraico se puede generalizar, al considerar un anillo R (en lugar de K) y un subanillo A del mismo (en lugar de Z). En este contexto se tienen las definiciones:

Definición 2.5 *Diremos que un elemento $r \in R$ es* **Entero sobre A**, *si r satisface un polinomio mónico con coeficientes en A.*

Definición 2.6 *Diremos que* **A es íntegramente cerrado en R**, *cuando todo elemento de R entero sobre A, pertenece a A.*

Ejemplo. Se puede verificar que el anillo de Enteros algebraicos de un cuerpo K es íntegramente cerrado sobre K.

Definición 2.7 *Un dominio A se dice que es* **íntegramente cerrado** *cuando es íntegramente cerrado en su cuerpo de fracciones.*

Definición 2.8 *Un dominio A se dice* **Dominio de Dedekind**, *cuando satisface las condiciones*

1. *A es un Anillo Noetheriano*
2. *A es íntegramente cerrado*
3. *Todo ideal primo, no nulo, de A es maximal*

Ejemplo. El anillo de enteros algebraicos de un cuerpo de números, es un Dominio de Dedekind (ver [17]).

Definición 2.9 *Sea A un dominio con cuerpo de fracciones K. Un* **Ideal fraccionario** *de A es un A-Módulo M, tal que $M \subseteq K$, y además existe un elemento $a \in A$, $a \neq 0$, tal que $aM \subseteq A$.*

A continuación enunciamos, sin demostración, el resultado más importante de la teoría de los dominios de Dedekind. Los detalles de la demostración se pueden ver en [17]

Teorema 2.9.1 (Teorema Fundamental de la teoría de Ideales) *Sea A un dominio. Entonces las siguientes condiciones son equivalentes:*

1. *A es un Dominio de Dedekind*
2. *Todo ideal no trivial de A se puede expresar en forma única como producto de ideales primos*
3. *El conjunto de los ideales fraccionarios no nulos de A, forman un grupo abeliano bajo el producto.*

3 Grupo de clases de ideales

Sea A un Dominio de Dedekind y K su cuerpo de fracciones. Sea $\mathcal{I}$ el grupo abeliano formado por los ideales fraccionarios de A y $\mathcal{P}$ el subgrupo formado por los ideales principales. Usando estas notaciones se tiene

Definición 3.1 *El* **Grupo de clases de ideales de K**, *o simplemente el grupo de clases de K, es el grupo cociente*

$$\mathcal{C}(\mathcal{K}) = \frac{\mathcal{I}}{\mathcal{P}}$$

Se puede probar que $\mathcal{C}(\mathcal{K})$ siempre es un grupo abeliano finito, cuando K es un cuerpo de números algebraicos. Esto no es cierto en general para Dominios de Dedekind.

Definición 3.2 *El* **Número de clases de K** *(Class number) de un cuerpo K de números algebraicos, el cual denotamos por h_K, es el orden del grupo finito $\mathcal{C}(\mathcal{K})$.*

Ejemplo. Sea $K = Q(\sqrt{-6})$, entonces se prueba fácilmente que el anillo de enteros correspondiente es de la forma

$$I_K = \left\{a + b\sqrt{-6}\right\}$$

El grupo de clases de ideales consta de dos elementos $\mathcal{C}(\mathcal{K}) = \{\mathcal{P}, \mathcal{C}\}$ donde $\mathcal{P}$ es la clase de los ideales principales y $\mathcal{C}$ es la clase con representante $\left(2, \sqrt{-6}\right)$.

Observación 2 *Es importante tener la mayor información posible acerca de la estructura de los ideales, en el anillo de enteros I_K, si se quiere conocer la factorización de un elemento cualquiera x, como producto de irreducibles. Si a es un elemento irreducible en I_K, entonces el ideal principal generado por a, no siempre es un ideal primo. Este hecho crucial en todo este trabajo, determina propiedades de factorización en estos anillos muy variadas, las cuales dependen en cierta forma del número de clases de ideales y de la estructura del grupo de clases.*
Si I_K es un dominio de factorización única, entonces esto si se puede garantizar para todo elemento irreducible a, esto es; su ideal principal es primo, y viceversa.

Para ilustrar lo antes dicho, veamos el ejemplo siguiente:

Ejemplo. En el anillo de enteros de $Q(\sqrt{-6})$ el elemento 2 es irreducible, sin embargo se tiene

$$(2) = (2, \sqrt{-6})^2$$

por lo tanto el ideal generado por 2 no es primo.
De igual forma se tiene, en este anillo

$$(3) = (3, \sqrt{-6})^2$$

con lo cual, el ideal (3) no es primo, aunque 3 es irreducible.
El discriminante de $Q(\sqrt{-6})$ es $d = 24$, y los únicos divisores primos son precisamente 2 y 3 . Estos son los únicos primos que **ramifican** en I_K. Se demuestra que si p es un primo diferente de 2 y 3 el cual no es solución de la ecuación $x^2 \equiv p \, mod \, 24$ entonces su ideal principal (p) es primo. Existen infinitos de ellos, por ejemplo $p = 7$.

4 Propiedades de factorización

Los Dominios de Dedekind en general no son Dominios de Factorización única. Esto ha sido observado desde el siglo pasado, al considerar el famoso ejemplo $I = Z + Z\sqrt{-5}$, en el cual se tiene

$$6 = 2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Se demuestra fácilmente que los elementos 2, 3, $(1 + \sqrt{-5})$ y $(1 - \sqrt{-5})$ son todos primos y ninguno de ellos es asociado de otro. Luego no hay factorización única en I.
Se puede demostrar que el anillo de enteros algebraicos de un cuerpo K es un Dominio de Factorización Unica si y sólo si su grupo de clases de ideales es el grupo trivial. Esto es, si y sólo si, $h_K = 1$.
Se penso durante mucho tiempo que el orden de h_K era una medida de que tan lejos se halla el anillo de enteros algebraicos I_K, de ser un Dominio de Factorización Unica.
Sin embargo no fue sino hasta 1960 que L.Carlitz [1] diera una interpretación cualitativa de este hecho. El probo que $h_K \leq 2$ si y sólo si el anillo de enteros

tiene la siguiente propiedad de factorización :
Si para algún x en I_K se tienen dos factorizaciónes en elementos irreducibles

$$x = a_1 a_2 .... a_r = b_1 b_2 .... b_t \tag{1}$$

entonces se debe tener $r = t$.
Un anillo con esta propiedad se denomina **anillo de factorización media.**

En 1969 Narkiewicz [13] propone caracterizar aritméticamente aquellos anillos de enteros algebraicos con $h_K \geq 3$. Desde entonces han aparecido una serie de resultados: Czogala [3], Kaczorowsky [9], Di Franco y Pace [6], Steffan J. L. [20] y D. Rush [18] entre otros.

En todos estos trabajos se dan algunas propiedades de factorización cuando $h_K \geq 3$. Sabemos que en estos anillos existen elementos x para los cuales $r \neq t$ en la ecuación 1.
Ahora bien, ¿ Qué tan grande es la diferencia $r - t$, o el cociente $\frac{r}{t}$?
El artículo de Zogala resuelve completamente esta pregunta para anillos con grupo de clases de ideales C(K) pequeños . Especifica mente para $C(K) = C_3$, $C_3 \oplus C_3$, C_4, $C_2 \oplus C_4$ y $C_2 \oplus C_2 \oplus C_2$, donde C_i es el grupo cíclico de orden i. En esta trabajo se da una generalización de estos resultados , usando un lema de combinatoria para grupos abelianos demostrado por J. Olson en 1969.
El artículo de J.L. Steffan, por otra parte, considera el cociente $\frac{r}{t}$ y da resultados de factorización mas generales. Veremos la relación entre ambos trabajos, la cual depende esencialmente de una constante asociada al grupo de clases G, la cual se denota por $D(G)$, y se llama constante de Davenport.
En la parte final de este sección, damos una caracterización de los anillos de enteros algebraicos con $D(G) = 5$, estos grupos son:

$$C_5, \quad C_3 \oplus C_3, \quad C_2 \oplus C_4 \quad y \quad C_2 \oplus C_2 \oplus C_2 \oplus C_2.$$

5 La constante de Davenport

Notación. Sea R un anillo de enteros del cuerpo de números K, con grupo de clases de ideales $G(K)$. Si P_i es un ideal de R, X_i indica la clase de este ideal en $G(K)$. El elemento neutro de este grupo lo denotamos por 1.

Proposición 1 *Sea a un elemento de R y supongamos que*

$$(a) = P_1 P_2 \dots P_n$$

con P_i ideales primos.
Entonces a es irreducible sí y sólo si para todo subconjunto de índices $\{i_1, \dots, i_k\}$ de $\{1, 2, \dots n\}$ con $1 \leq k < n$

$$X_{i_1} X_{i_2} \dots X_{i_k} \neq 1 \tag{2}$$

Demostración. Supongamos que existe $\{i_1, \dots, i_k\} \subset \{1, \dots, n\}$ con $k < n$ y tal que

$$X_{i_1} \dots X_{i_k} = 1$$

Entonces el ideal $X_{i_1} \dots X_{i_k}$ es principal, luego existe un elemento b en R tal que

$$(b) = X_{i_1} ... X i_k$$

El ideal (b) divide al ideal (a) luego $a = b.c$, para algún c en R. Como a es irreducible c debe ser unidad. Luego $(b) = (a)$ y por lo tanto

$$X_{i_1} \dots X_{i_k} = (b) = (a) = X_{i_1} \dots X_{i_n}$$

Como la factorización de ideales es única, se debe tener $n = i_k$, lo cual es una contradicción.

Por otro lado, supongamos que a no es irreducible, entonces a = b.c, con b y c en R no unidades. Luego

$$P_1 \dots P_n = (a) = (b)(c)$$

lo cúal implica (b) $= P_{i_1} \dots P_{i_k}$, con $\{i_1, ..., i_k\} \subset \{1, ...n\}$ y $k < n$. Por lo tanto

$$1 = X_{i_1} ... X_{i_k}$$

con $k < n$, lo cual contradice 2

A continuación daremos una definición de una constante asociada a un grupo abeliano finito G, la cual esta relacionada con la condición 2 del teorema anterior.

Definición 5.1 *Sea G un grupo abeliano finito, entonces $D(G)$ es es el menor entero positivo s tal que para todo conjunto de elementos $g_1, \ldots, g_t$ en G, con $t \geq s$ se tiene que existen subíndices $\{i_1, \ldots, i_k\} \subset \{1, \ldots, t\}$ tales que*

$$g_{i_1} \ldots . g_{i_k} = 1.$$

Este entero $D(G)$ se llama **Constante de Davenport.**

En 1966 H. Davenport destaco la conexión de esta constante con la teoría de los números algebraicos (Conferencia de Teoría de Números y teoría de grupos del medio Oeste, Universidad de Ohio). El problema de determinar la misma fue atacado por H.Olson, Mann y otros (ver [15], [16], [11]). Recientemente, Geroldinger y Schneider (ver [7]) han estudiado nuevas propiedades de la misma y su relación con otras áreas de la matemática.

Proposición 2 *Si el orden de G es n, entonces $1 \leq D(G) \leq n$*

Demostración Sean $g_1, \ldots . g_t \in G$ con $t \geq n$. Entonces los elementos

$$x_1 = g_1, \quad x_2 = g_1 g_2, \quad \ldots . \quad x_t = g_1 g_2 \ldots . g_t$$

son t elementos en G.
Luego por ser $t \geq n$ debemos tener algunos de ellos repetidos, digamos $x_i = x_j$ con $i < j$ luego

$$g_1 \cdots g_i = g_1 \cdots g_i g_{i+1} \cdots g_j$$

de donde $g_{i+1} \ldots g_j = 1$. Luego tenemos $j - i$ elementos de G (distintos de la identidad) y cuyo producto es la identidad. Luego $D(G) \leq n$.

Proposición 3 *Si G es un grupo cíclico de orden n, se tiene $D(G) = n$.*

Demostración Sea G el grupo cíclico generado por g. Entonces la sucesión de elementos $g, g, \ldots, g$ (n veces) no tiene subsucesión cuyo producto sea la identidad, lo cual implica $D(G) \geq n$. Usando ahora el teorema anterior se concluye la demostración.

El siguiente resultado se debe a J.Olson [15]

Teorema 5.1.1 *Sea G un grupo abeliano de la forma*

$$G = C_{p^{e_1}} \oplus .... \oplus C_{p^{e_r}}$$

con p_i números primos. Entonces

$$D(G) = 1 + \sum_{i=1}^{r}(p^{e_i} - 1)$$

Si G es un producto directo de grupos cíclicos

$$G = C_{m_1} \oplus ... \oplus C_{m_s}$$

entonces para cada i, $1 \leq i \leq s$ tomemos el elemento $x_i = (0, 0, \ldots, 1, \ldots 0)$ de orden m_i. Entonces el conjunto de elementos $x_1, ...x_1, ..., x_{m_s}$, donde cada x_i aparece repetido $m_i - 1$ veces, no posee subconjunto cuyo producto sea la identidad. Por consiguiente

$$D(G) \geq \sum_{i=1}^{s} m_i - s + 1$$

La desigualdad anterior parece ser una igualdad. Sin embargo existe una gran cantidad de grupos en donde esto falla. Por ejemplo (ver [7]) $G = C_3 \oplus C_3 \oplus C_3 \oplus C_6$, para el cual se tiene :

$$D(G) > (2 + 2 + 2 + 5) + 1$$

No se sabe si existe algún otro ejemplo de rango 3.
En el caso especial s= 2, se tiene la igualdad (Ver [15] para la demostración).

Teorema 5.1.2 *Sea $G = C_m \oplus C_n$ con C_i grupo cíclico de orden i y $m \mid n$. Entonces se tiene*

$$D(G) = m + n - 1$$

Existen muchos grupos con el mismo número de Davenport. Mas precisamente, si n es suficientemente grande entonces habrá muchos grupos G, con constante de Davenport igual a n. El siguiente resultado nos da un buen estimado de la cantidad de grupos con esta propiedad.

Teorema 5.1.3 *Sea n un entero positivo* $n \geq 2$. *Entonces existen* $[\frac{n+5}{3}]$ *grupos G, con D(G) = n.*

Demostración En primer lugar si G = C_n se tiene D(G) = n. Veamos que hay otros grupos, además de este, con la propiedad D(G) = n.
Sean h y k enteros y consideremos

$$G = C_2^h \oplus C_4^k.$$

Entonces si hacemos h + 3k + 1 = n, se tendrá D(G) = n. Luego, los posibles valores de k son $0, 1, \ldots, [\frac{n-1}{3}]$, lo cual nos da $[\frac{n+2}{3}]$ posibilidades para G. Si además incluimos el grupo cíclico de orden n, entonces se obtiene el resultado.

6 El número mediador

Existe otra constante asociada a un grupo abeliano finito G, llamada el **Número Mediador** (Cross number, ver Krause), el cual relaciona propiedades de factorización en el Anillo de enteros algebraicos y su grupo de clases de ideales. Dicho número esta relacionado con la constante de Davenport y estudiaremos a continuación algunas de sus propiedades mas relevantes.

Definición 6.1 *Sea G un grupo abeliano finito. Una n-upla* $(g_1, g_2, \ldots g_n)$ *de elementos de G, no necesariamente distintos, se dice* **Sistema Mínimal** *si*
i) $g_1 \ldots g_n = 1$
ii) $g_{i_1} \ldots g_{i_s} \neq 1$ *para todo* $1 \leq s < n$.

Observación 3 *Es claro que en la definición anterior, ningún elemento de la n-upla puede ser igual a la identidad del grupo. Si esto ocurre, se tendrá un subproducto formado por un solo elemento el cual es igual a uno. Esto naturalmente, contradice la definición.*

Podemos redefinir la constante de Davenport D(G), usando el concepto de Sistema Minimal

Definición 6.2 *Sea G un grupo abeliano finito, entonces*

$$D(G) = Max\{n/(g_1, \ldots, g_n) \ \ sistema\ minimal\}$$

Definición 6.3 *Sea G un grupo abeliano finito. Definimos el* **número mediador de** *G, como*

$$K(G) = Max\left\{\sum_{i=1}^{r} \frac{1}{ordg_i} \mid (g_1, \ldots, g_r) \text{ sistema minimal}\right\}.$$

Proposición 4 *El número mediador K(G) de un grupo G satisface*

$$1 \leq K(G) \leq \|G\|$$

Demostración Sea $g \in G$,$g \neq e$ y s = ord (g). Luego $(g, \ldots, g)$ (s veces) es un sistema minimal de G , y además

$$\sum_{i=1}^{s} \frac{1}{ord(g)} = 1$$

luego $K(G) \geq 1$.

Por otro lado , si $(g_1, \ldots, g_s)$ es un sistema minimal cualquiera se tiene siempre que $s \leq \|G\|$ con lo cual obtenemos

$$\sum_{r=1}^{s} \frac{1}{ord(g_i)} \leq \sum_{i=1} s1 = s \leq \|G\|$$

En algunos casos es posible obtener una formula explícita para K(G) .

Teorema 6.3.1 *Sea G un grupo abeliano de la forma*

$$G = C_p \oplus \ldots \oplus C_p$$

con n copias de C_p. *Entonces*

$$K(G) = \frac{np + 1 - n}{p}$$

Demostración De acuerdo a la definición se tiene

$$\begin{aligned} K(G) &= max\left\{\sum_{i=1}^{s}\frac{1}{ordg_i}|(g_1,\ldots g_s)\text{sistema minimal}\right\} \\ &= \frac{1}{p}max\left\{\sum_{i=1}^{s}1|(g_1,\ldots,g_s)\text{sistema minimal}\right\} \\ &= \frac{D(G)}{p} \\ &= \frac{1+\sum_{i=1}^{n}p-1}{p} \\ &= \frac{np+1-n}{p} \end{aligned}$$

Proposición 5 *Sea p un primo cualquiera, entonces existe un grupo G abeliano finito, tal que*

$$K(G) = p$$

Demostración Aplicar el teorema anterior para el caso n = p + 1.

El número mediador K(G) de un grupo finito abeliano G, es una medida de la desviación de los ordenes de los elementos de G con respecto al orden del grupo . El siguiente teorema es una muestra de ello. (Ver Krause)

Teorema 6.3.2 *Un grupo abeliano G finito, es cíclico de una potencia de un primo si y solo si K(G) = 1.*

Finalmente, daremos un resultado interesante en relación a los sistemas minimales en un grupo cíclico de orden p, el cual usaremos en la próxima sección.

Teorema 6.3.3 *Sea G un grupo finito cíclico de orden p . Entonces si* $(g_1,\ldots,g_p)$ *es un sistema minimal se tiene* $g_1 = g_2 = \ldots = g_p$.

Demostración Sea $(g_1,\ldots,g_p)$ un sistema minimal. Podemos asumir que hay al menos dos elementos diferentes, digamos g_{p-2} y g_{p-1} . Luego se tienen los siguientes elementos en G

$$\begin{aligned} x_1 &= g_1 \\ x_2 &= g_1g_2 \end{aligned}$$

$$\begin{aligned} &\vdots \\ x_{p-2} &= g_1 g_2 \cdots g_{p-2} \\ x_{p-1} &= g_1 \cdots g_{p-3} g_{p-1} \\ x_p &= g_1 \cdots g_{p-3} g_{p-2} g_{p-1} \end{aligned}$$

Tenemos entonces p elementos del grupo G, ninguno de los cuales es igual a la identidad. Luego debe haber alguno repetido, esto por supuesto nos conduce a una ecuación del tipo

$$g_{i_1} \cdots g_{i_t} = 1 \quad con \quad 1 \leq i < p$$

lo cual es una contradicción. Por lo tanto $g_1 = g_2 = \ldots = g_p$

7 Propiedades de factorización

A continuación daremos una serie de definiciones y teoremas, siguiendo de cerca los artículos de Czogala y Steffan. Muchos de estos resultados son ciertos para Dominios de Dedekind en general, otros sin embargo, sólo se cumplen en anillos de enteros algebraicos de un cuerpo de números.

Definición 7.1 *Sea R un Dominio de Dedekind y $n \geq 1$. Diremos que R satisface la propiedad T_n, si para todo elemento a irreducible en R se tiene*

$$(a) = P_1 \ldots . P_k$$

con P_i ideales primos y $k \leq n$.

Definición 7.2 *Sea R un Dominio de Dedekind, entonces la* **Profundidad de R**, *denotada por $T(R)$ es el número natural*

$$T(R) = min\{n | R\ satisface\ T_n\}$$

Observación 4 *Si R es Dominio de Dedekind, de acuerdo a la definición de la constante de Davenport, se tendrá $T(R) \leq D(G)$, donde G es el grupo de clases de R.*

Teorema 7.2.1 *Sea R anillo de enteros algebraicos de un cuerpo de números K, entonces*

$$T(R) = D(G)$$

.

Demostración En efecto, sea $(X_1,,,,X_{D(G)})$ un sistema minimal en G. Entonces es posible tomar un ideal primo en cada una de estas clases, ver [13]. Sean entonces los ideales primos P_i pertenecientes a las clases X_i. Luego existe un irreducible a tal que

$$P_1....P_{D(G)} = (a)$$

por lo tanto $T(R) \geq D(G)$. Con esto se concluye la prueba.

Definición 7.3 *(Czogala) Sea n un número entero $n \geq 2$. Diremos que el Dominio R satisface la* **propiedad** V_n *si para cualquier conjunto de elementos irreducibles $a_1, a_2, b_1, b_2, ..., b_k$ de R la igualdad*

$$a_1 a_2 = b_1 b_2 .... b_k$$

implica $k \leq n$.

Ejemplo Si R es un dominio de factorización única entonces, entonces R satisface V_2.

Definición 7.4 *Sea R un dominio, definimos la constante $V(R)$ de la forma*

$$V(R) = min\{V_n | R \quad satisface \quad V_n\}$$

Proposición 6 *Sea R un Dominio de Dedekind. Entonces R satisface $V(R) \leq D(G)$.*

Demostracion Sean $a_1, a_2, b_1, b_2, ..., b_k$ elementos irreducibles de R y supongamos que $a_1 a_2 = b_1 \dots b_k$. Debemos probar $k \leq n$.
Tomando los ideales generados por estos elementos obtenemos

$$(a_1)(a_2) = (b_1)(b_2) \dots (b_k) \tag{3}$$

Usando el teorema fundamental de los Dominios de Dedekind para R, se tiene que cada ideal se descompone de manera unica como un producto de ideales primos. Consideramos entonces los casos:

1) Si alguno de los ideales (a_i), (b_j) es primo, digamos (a_1) es primo, entonces este ideal aparece en el lado izquierdo de la ecuación 3 y por lo tanto (a_1) divide a alguno de los ideales $(b_1), (b_2), \ldots, (b_k)$.
Si (a_i) divide a (b_j), digamos, entonces $b_i = a_1.unidad$, luego podemos cancelar este ideal en la ecuación 3 para obtener

$$a_2.unidad = b_1 ... b_{j-1} b_{j+1} ... b_k$$

como a_2 es irreducible debemos tener un solo elemento irreducible del lado derecho y por lo tanto $k = 2 \leq n$.

2) Si ninguno de los ideales principales es primo, sea (a_i) producto de n_i ideales primos $1 \leq i \leq 2$. De la misma forma, sea (b_j) producto de m_j ideales primos $1 \leq j \leq k$. Luego debemos tener $n \geq n_j \geq 2$ y $n \geq m_j \geq 2$. Por otro lado , contando los ideales primos en ambos miembros de 3 , tenemos

$$2n \geq n_1 + n_2 = m_1 + m_2 + ... + m_k \geq 2k$$

de donde $k \leq n$.

A continuacion daremos otra definición , dada por L. Steffan la cual relaciona las posibles longitudes de factorización de un elemento de R.

Definición 7.5 *(Steffan) Sea q un número racional* $q \geq 1$. *Diremos que R satisface la propiedad* E_q *si para todos elementos irreducibles* $a_1, \ldots, a_r, b_1, \ldots, b_s$ *en R , con*

$$a_1 \ldots a_r = b_1 \ldots b_r$$

se tiene entonces $\frac{1}{q} \leq \frac{r}{s} \leq q$.

Definición 7.6 *Sea R un dominio. Entonces se define la constante* $E(R)$ *de la siguiente forma*

$$E(R) = min\{E_q | R \quad satisface \quad E_q\}$$

Teorema 7.6.1 *Sea $n \geq 1$ un entero, y R un dominio de Dedekind , entonces*

$$T(R) \leq \frac{1}{2}E(R) \leq V(R)$$

Demostración ($T_n \Rightarrow E_{n/2}$)
Sean $a_1, \ldots, a_r$, y $b_1, \ldots, b_s$ elementos irreducibles (no primos) de R y supongamos que

$$a_1 \ldots a_r = b_1 \ldots b_s,$$

luego tomando ideales

$$(a_1) \ldots (a_r) = (b_1) \ldots (b_s)$$

Cada (a_i) es un producto de a lo sumo n ideales primos. Por otro lado, cada (b_j) es un producto de dos o mas ideales primos. Luego contando el número de ideales en la expresión anterior se tiene $2s \leq rn$, de donde se concluye $\frac{s}{r} \leq \frac{n}{2}$. Es decir R tiene la propiedad $E_{\frac{n}{2}}$

$(E_{\frac{n}{2}} \Rightarrow V_n)$
Sean $a_1, a_2, b_1, \ldots b_k$ elementos irreducibles tales que

$$a_1 a_2 = b_1 \ldots b_k$$

luego $\frac{k}{2} \leq \frac{n}{2}$, de donde $k \leq n$.
Por lo tanto el ideal R satisface la propiedad V_n.

Teorema 7.6.2 *Si R es un anillo de enteros de un cuerpo de números se tiene*

$$T(R) = \frac{1}{2}E(R) = V(R)$$

Demostracion Probaremos $V_n \Rightarrow P_n$.
Sea $(a) = P_1 \ldots P_k$. Sea X_i la clase de P_i, y tomemos $Q_i \in X_i^{-1}$. Luego existen irreducibles b_i, $1 \leq i \leq k$ y b tales que $(b_i) = P_i Q_i$, $(b) = Q_1 \ldots Q_k$. Luego

$$\begin{aligned} (ab) &= P_1 \ldots P_k Q_1 \ldots Q_k \\ &= P_1 Q_1 \ldots P_k Q_k \\ &= (b_1) \ldots (b_k) \end{aligned}$$

Por lo tanto

$$ab = b_1 \dots b_k \quad \text{salvo unidades}$$

luego debe ser $k \leq n$. Con lo cual se ha demostrado que R satisface P_n.

8 Anillos con Constante de Davenport igual a cinco

En [3] estan caracterizados todos los anillos de enteros con grupo de clases G , tales que $1 \leq D(G) \leq 4$. Estos son los siguientes:

$$C_2, \quad C_3, \quad C_2 \oplus C_2, \quad C_2 \oplus C_2 \oplus C_2 \quad y \quad C_4$$

En esta sección daremos una caracterización para anillos de enteros algebraicos con grupo de clases de ideales G, tales que D(G) = 5. Estos son

$$C_5 \quad , C_3 \oplus C_3, \quad C_2 \oplus C_2 \oplus C_2 \oplus C_2 \quad y \quad C_2 \oplus C_4$$

. Comenzaremos estableciendo una propiedad de factorización en el anillo de enteros algebraicos R, la cual es fundamental en todo este trabajo.

Definición 8.1 *Sea a un elemento irreducible en R. Entonces para todo* $n \geq 1$ *se define* $S_n(a)$ *como el mayor entero k, tal que* $a^n = b_1 \dots . b_k$, *donde* $b_1, \dots, b_k$ *son elementos irreducibles en R.*

Definición 8.2 *Sea* $n \geq 1$. *Sea define* $S_n(R)$ *como el máximo de los* $S_n(a)$ *con a irreducible en R.*

Teorema 8.2.1 *Si R es un anillo de enteros con* $G = C_5$, *entonces*

$$S_2(R) = 2$$

Demostracion Claramente se tiene $S_2(R) \geq 2$. Probaremos que $S_2(a) \leq 2$ para todo irreducible a.
Supongamos que existen ideales primos $P_1, \dots, P_t$, tales que

$$(a) = P_1 \dots P_t \tag{4}$$

con $2 \leq t \leq 5$.

Supongamos que $a^2 = b_1....b_k$, con b_i irreducibles. Luego

$$(a)^2 = (b_1)....(b_k) = P_1^2 \dots P_t^2 \tag{5}$$

Sea m_i = número de ideales primos en la factorización del ideal (b_i). Probaremos que $k \leq 2$, para lo cual tendremos que que considerar todos los posibles valores de t en 4

Si t = 5, entonces probaremos que $P_1, \dots, P_5$ estan en la misma clase en G. Sean $X_1, \dots, X_5$ las clases correspondientes de estos ideales en G. Entonces el sistema $(X_1, \dots, X_5)$ es un sistema minimal en G, y de acuerdo al teorema 6.3.3 se tendrá que todos los X_i son iguales. Es decir, todos los ideales primos P_i estan en una misma clase X en G.

Asi tendremos en 5

$$(b_1) \dots (b_k) = P_1^2 \dots P_5^2$$

luego, debe ser $m_i = 5$ para todo i, y por lo tanto k = 2.

Si $3 \leq t \leq 4$ en 4, entonces el número de ideales primos en la factorización de cada uno de los (b_i) en 5, el cual hemos denotado por m_i, es mayor o igual a 3.
En efecto, basta observar que no se puede tener $(b_i) = P^2$ o bien $(b_i) = PQ$, si P y Q son ideales primos en la factorización de (a). Por lo tanto $m_i \geq 3$ para todo i .
Luego , podemos contar los ideales primos en ambos lados de 5 para obtener

$$2t = \sum_{i=1}^{k} m_i \geq 3 \sum_{i=1}^{k} 1 = 3k$$

de donde $k \leq 2$.

Si t= 2 la demostracion es trivial.

Observación 5 *L. Salce y P.Zanardo , ver [19], Demostraron, usando otros métodos que $S_2(R) = 2$, si y sólo si el grupo de clases de ideales de R, es cíclico de orden 2, 3, 4, 5 y 7.*
Pregunta 1: ¿ Para que anillos R se tiene $S_2(R) \leq 3$?
Pregunta 2: ¿ Para que anillos R se tiene $S_3(R) \leq 3$?

Teorema 8.2.2 *Sea R anillo de enteros con grupo de clases*

$$G = C_2 \oplus C_2 \oplus C_2 \oplus C_2.$$

Entonces $S_2(R) = 5$

Demostración Sea a en R un elemento irreducible, y supongamos

$$(a) = P_1.....P_t, \quad con \quad 1 \leq t \leq 5$$

. Supongamos que existen elementos irreducibles $b_1, \ldots, b_k$ tales que

$$a^2 = b_1....b_k$$

Luego

$$(a)^2 = P_1^2.....P_t^2 = (b_1).....(b_k)$$

Notemos, en primer lugar que todos los elementos de G son de orden dos. Por lo tanto los ideales primos P_1 ,..., P_t estan todos en clases diferentes.

Las posibilidades para (b_i) son

1. $(b_i) = P_i^2$
2. $(b_i) = P_1^{\alpha_1}....P_t^{\alpha_t}$

con $\sum_{i=1}^{t} \alpha_i \geq 3$.
Tenemos entonces, nuestra ecuación fundamental:

$$10 \geq 2t = \sum_{i=1}^{k} m_i \geq 2\sum_{i=1}^{k} 1$$

de donde $k \leq 5$ y por lo tanto $S_2(R) \geq 5$.

Por otro lado es fácil ver que $S_2(R) \geq 5$. Consideremos los elementos en G, $x_1 = (1,0,0,0)$ $x_2 = (0,1,0,0)$ $x_3 = (0,0,1,0)$ $x_4 = (0,0,0,1)$ y $x_5 = (1,1,1,1)$ y sean P_i ideales primos en cada clase x_i. Luego existen elementos irreducibles a, b_i tales que:

$$(a) = P_1 \ldots P_5, \quad (b_i) = P_i^2$$

por lo tanto

$$(a)^2 = P_1^2 \ldots P_5^2 = (b_1) \ldots (b_5)$$

De donde $S_2(R) \leq 5$.

Teorema 8.2.3 *Sea R anillo de enteros con grupo de clases*

$$G = C_2 \oplus C_4$$

Entonces $S_2(R) = 3$.

Demostración Como siempre, sea a irreducible en R y supongamos que a tiene una descomposicion en ideales primos

$$(a) = P_1 .... P_t$$

Supongamos además que

$$a^2 = b_1 .... b_k$$

con b_i elementos irreducibles en R. Luego se tiene la ecuación fundamental

$$(a)^2 = P_1^2 .... P_t^2 = (b_1) \dots (b_k)$$

Los posibles tipos de ideales (b_i) son los siguientes:

- $A \quad (b_i) = P_j^2$
- $B \quad (b_i) = P_1^{\alpha_1} \dots P_t^{\alpha_t} \quad \alpha_1 + \dots + \alpha_t = 3$
- $C \quad (b_i) = P_1^{\alpha_1} .... P_t^{\alpha_t} \quad \alpha_1 + ... + \alpha_t = 4$
- $D \quad (b_i) = P_1^{\alpha_1} \dots P_t^{\alpha_t} \quad \alpha_1 + \dots + \alpha_t = 5$

Nótese que en G solo hay tres elementos de orden 2 : $x_1 = (1,0)$, $x_2 = (1,2)$ y $x_3 = (0,2)$. Ademas se tiene $x_1.x_2.x_3 = E$. Luego en el conjunto $\{P_1, \dots P_t\}$ hay a lo sumo dos ideales cuyas clases sean de orden dos.
Si t=5, entonces hay un solo ideal P_i cuya clase es de orden dos. En efecto, algún subproducto de $P_3.P_4.P_5$ es de orden dos, luego no pueden estar P_1 y P_2 en clases de orden dos. Por lo tanto sólo puede haber un ideal del tipo A.

Entonces, contando el número total de ideales (b_i) tenemos

$$10 = \sum_{i=1}^{k} m_i \geq 2 + 3 \sum_{i=2}^{k} 1$$

de donde $k \leq 3$.

Si t=4 entonces hay a lo sumo dos ideales (b_i) del tipo A. Luego

$$8 = \sum_{i=1}^{k} m_i \geq 4 + 3\sum_{i=3}^{k} 1$$

de donde nuevamente, $k \leq 3$.

Si $2 \leq t \leq 3$ es fácil verificar que $k \leq 3$. Por lo tanto $S_2(G) \leq 3$.

Para demostrar la otra desigualdad, consideremos los elementos del grupo G

$$x_1 = (1,0),\ x_2 = (0,1),\ x_3 = (1,1)$$

. Sean P_i ideales primos pertenecientes a las clases x_i. Luego existen elementos irreducibles a $b_1, \ldots, b_4$ tales que

$$(a) = P_1P_2^3P_3 \quad (b_1) = P_1^2 \quad (b_2) = P_2^4 \quad (b_3) = P_2^2P_3^2.$$

Luego

$$(a)^2 = P_1^2P_2^6P_3^2 = (b_1)(b_2)(b_3)$$

de donde $S_2(R) \geq 3$.

Teorema 8.2.4 *Si el anillo de enteros tiene grupo de clases*

$$G = C_3 \oplus C_3,$$

entonces $S_2(R) = 3$.

Demostración Sea a un elemento de R, irreducible y sea

$$(a) = P_1 \ldots P_t$$

P_i ideales primos y $1 \leq t \leq 5$.
Supondremos que $a^2 = b_1 \ldots b_k$ y entonces tendremos la ecuación fundamental en ideales

$$P_1^2 \ldots P_t^2 = (b_1) \ldots (b_k)$$

Las posibilidades para (b_i), que hacen el valor de k máximo son

$$(b_i) = P_j^3 \quad o \quad (b_i) = P_j^2P_l$$

Por lo tanto $m_i \geq 3$ para todo i .

Contando los ideales en ambos lados de la ecuación fundamental tenemos

$$10 \geq 2t = \sum_{i=1}^{k} m_i \geq 3 \sum_{i=1}^{k} 1$$

lo cual nos da $k \leq 3$, y de aqui concluimos $S_2(R) \geq 3$.
Probaremos ahora que este valor extremo es alcanzado. Para la demostración tomamos las clase de ideales

$$X_1 = (1,0)\ X_2 = (0,1)\ X_3 = (1,1)$$

de $G = C_3 \oplus C_3$
Sean P_i $1 \leq i \leq 3$, ideales primos pertenecientes a X_i. Luego existen elementos irreducibles a, b_i $1 \leq i \leq 3$ tales que

$$P_1^2 P_2^2 P_3 = (a)\ P_1^3 = (b_1)\ P_2^3 = (b_2)\ P_1 P_2 P_3^2 = (b_3)$$

luego

$$(a)^2 = P_1^4 P_2^4 P_3^2 = (b_1 b_2 b_3)$$

Por lo tanto $S_2(R) \geq 3$. Con esto termina la demostración.

Observación 6 *Hemos visto que $S_2(R) = 3$ cuando R tiene grupo de clases: $C_3 \oplus C_3$ o bien $C_2 \oplus C_4$, ambos grupos tienen número de Davenport igual a 5. Luego la constante de Davenport D(G) y el número $S_2(R)$ no son suficientes para caracterizar G.*

Nuestro objetivo siguiente, será calcular los valores de $S_n(R)$, para los dos grupos de arriba, a fin de poder diferenciar ambos, en cuanto a propiedades aritméticas.
Comenzaremos por considerar un elemento a irreducible en R y (a) el ideal principal generado por éste, el cual se factoriza como producto de t ideales primos con $1 \leq t \leq 5$. Entonces el ideal generado por a^n se factoriza como producto de tn ideales primos. Es claro entonces que el número k de elementos irreducibles en la factorización de a^n es máximo, cuando tn es máximo. Por este motivo tomaremos t = 5 en la ecuación fundamental , lo cual nos da el máximo valor de tn.

Comenzaremos con el estudio del grupo $G = C_3 \oplus C_3$. Es fácil demostrar que si (a) es producto de 5 ideales primos, entonces debe ser de la forma

$$(a) = P_1^2 P_2^2 P_3$$

con P_i primos.
Si suponemos que $a^n = b_1 \dots b_k$, entonces contando los ideales en la ecuación fundamental de a^n nos produce

$$5n = \sum_{i=1}^{k} m_i = 3b + 4c + 5d$$

donde b, c y d es el número de ideales de los tipos B, C y D respectivamente. Además se tiene la condición $b + c + d = k$. Nuestro plan, será entonces hallar, para cada n, el valor máximo de k que satisface las ecuaciones

$$5n = 3b + 4c + 5d$$

$$k = b + c + d$$

Esto viene expresado en la siguiente tabla

n	b	c	d	k
2	2	1	0	3
3	5	0	0	5
4	5	0	1	6
5	7	1	0	8
6	10	0	0	10
7	10	0	1	11
8	12	1	0	13

Seguidamente tratamos el caso en que $G = C_2 \oplus C_4$. Nuevamente sea a un elemento irreducible y supondremos que el ideal principal generado por él es producto de 5 ideales primos. Se puede demostrar entonces que (a) es de la forma

$$(a) = P_1 P_2^3 P_3$$

donde P_1 es de orden 2 y P_2 y P_3 son de orden 4. Si suponemos que $a^n = b_1 \dots b_k$, entonces contando los ideales en la ecuación fundamental nos da

$$5n = \sum_{i=1}^{k} m_1 = 2a + 3b + 4c + 5d$$

donde a, b, c, c, y d es el número de ideales de los tipos A, B, C y D que aparecen en la factorización de $(a)^n$. Es de notar, que los números a y b estan limitados , dado que sólo hay un ideal de orden dos. Luego se tiene: $a \leq [n/2]$. También b depende de a puesto que para formar un ideal del tipo B, se necesita un ideal de orden dos.
Al igual que antes, nuestro problema se reduce a calcular el valor de k máximo, sujeto a las condiciones

$$5n = 2a + 3b + 4c + 5d$$

$$k = a + b + c + d$$

estos valores los representamos en la siguiente tabla

n	a	b	c	d	k
2	1	0	2	0	3
3	1	3	1	0	5
4	2	0	4	0	6
5	0	5	0	2	7
6	3	0	6	0	9
7	3	0	6	1	10
8	4	0	8	0	14

A manera de ejemplo, demostraremos que $S_5(R) = 7$ cuando R tiene grupo de clases de ideales $G = C_2 \oplus C_4$.
Sean $x_1 = (1,0)$, $x_2 = (0,1)$ y $x_3 = (1,1)$ en G, y P_i ideales primos en cada una de estas clases. Luego existen irreducibles a, b_1, b_2, b_3 tales que

$$(a) = P_1 P_2^2 P_3 \ (b_1) = P_1^2 \ (b_2) = P_2^4 \ (b_3) = P_3^4$$

luego

$$\begin{aligned} (a^5) &= P_1^5 P_2^{15} P_3^5 \\ &= (P_1^2)^2 (P_2^4)^3 (P_3^4) P_1 P_2^2 P_3 \\ &= (b_1^2 b_2^3 b_3 a) \end{aligned}$$

de donde $S_5(R) \geq 7$. Luego $S_5(R) = 7$.

También se puede probar que $S_5(R) = 8$ cuando R tiene grupo de clases de ideales $C_3 \oplus C_3$.
En efecto, basta tomar los elementos en el grupo G

$$x_1 = (1,0)\ x_2 = (0,1)\ x_3 = (1,1)$$

y P_i ideales primos en cada una de esas clases. Luego existen elementos irreducibles

$$(b_1) = P_1^3\ (b_2) = P_2^3\ (b_3) = P_3^3\ (b_4) = P_1 P_2 P_3^2$$

Luego

$$\begin{aligned}(a^5) &= P_1^{10} P_2^{10} P_3^5 \\ &= P_1^9 P_2^9 P_3^3 P_1 P_2 P_3^2 \\ &= (b_1^3 b_2^3 b_3 b_4)\end{aligned}$$

con esto se demuestra $S_5(R) = 8$.

Teorema 8.2.5 *Sea R es anillo de enteros con grupo de clases G , entonces*
1) Si $G = C_3 \oplus C_3$, *se tiene* $S_5(R) = 8$
2) Si $G = C_2 \oplus C_4$, *entonces se tiene* $S_5(R) = 7$.

Bibliografía

[1] L. Carlitz A characterization of algebraic fields with class number two, Proc.Amer.Math.Soc. 11 (1960) 391-392

[2] L. Claborn Every Abelian Group is a class Group Pacific J.Math.18 (1966) , 219-222.

[3] A.Czogala Arithmetic characterization of algebraic number fields with small class numbers. Math.Z. 176 (1981) , 247-253.

[4] S. Chapman A simple example of non-unique factorization in Integral Domain. Amer.Math.Month. Dec. 1992 , p.943

[5] S.Chapman y W.Smith On a characterization of algebraic number fields with class number less than three. J. of Algebra 135,(1990) p 381-387.

[6] Di Franco y F.Pace. Arithmetical characterization of rings of algebraic Integers with class number three and four. Bolletino U.M.I. Algebra e Geometria Serie VI , volV D.N.1 (1985)

[7] A.Geroldinger y R.Schneider . On Davenport's Constant J. of Combinatorial theory vol.61 No 1 , September 1992

[8] K.Ireland y M.Rosen A classical introduction to Modern Number Theory . Springer Verlag, New York - 1982.

[9] J. Kaczorowski A pure arithmetical definition of the class group. Colloq.Math. vol 48 , 1984.

[10] Krause Ulrich . A characterization of Algebraic Number Fields with Ciclic Class Group of prime power Order. Mathh. Z. 186. 143-148 . 1984.

[11] .H.Mann- Additive group Theory - A Progress Report Bull. of the Amer. Math. Soc. vol79. Number 6. November 1973.

[12] D.Michel y J.L.Steffan Repartitions des ideaux premiers parmi les clases d'ideaux d'un anneau de Dedekind. J. Algebra , 98 (1986) , 82-94.

[13] W. Narkiewicz Elementary and Analityc Theory of Algebraic Numbers. Warszawa : PWW -Polish Scientific Publishers 1974.

[14] W.Narkiewicz Some unsolved Problems Bull.Soc.Math.France 25 (1971) p 159-164.

[15] J.E. Olson A combinatorial Problem on Finite Abelian Groups,I J.Number Theory 1 , 1969 p 8-10

[16] J.E. Olson A combinatorial problem on Finite Abelian Groups ,II J. Number Theory 1, (1969) p. 195-199

[17] Roy Quintero .Caracterizacion de anillos de Enteros algebraicos en terminos del número de clases de ideales. Tesis de Maestria. Univ. de Los Andes , Merida (1991)

[18] D.Rush An arithmetic characterization of algebraic number fields with a given class group. Math.Proc.Camb.Phil.Soc. (1983) 94 , 23.

[19] L. Salce y P. Zanardo . Arithmetical Characterization of rings of algebraic integers with cyclic ideal class group. Bolletino U.M.I. Algebra e Geometría Serie VI, vol.I- D.N.1. 1982

[20] J.L.Steffan Longueurs des decompositions en produits d'elements irreductibles dans un anneau de Dedekind. J. of Algebra 102 (1986)

[21] R.J. Valenza . Elasticity of factorization in Number Fields Journal of Number theory , 36. 212-218 (1990)

[22] A. Zaks Half-Factorial-Domains Israel J. of Math. vol37 No4 (1980)

[23] A. Zaks Half- FactoriaL- Domains Bull. of the Amer.Math.Soc. vol. 82 , number 5, (1976)