ANILLOS DE DIVISION

por

MARÍA J. WONENBURGER

INTRODUCCION

Este artículo tiene por objeto presentar algunos resultados de la teoría de anillos de división y ofrecer al lector una descripción de las contribuciones de diversos autores que han ideado métodos para la construcción de ejemplos de cuerpos no conmutativos.

Los números entre corchetes se refieren a la bibliografía que aparece al final en la que se da la referencia de los libros o artículos en los que el lector puede encontrar las construcciones mencionadas en el texto. La lectura de tales artículos no presenta grandes dificultades. Para un estudio completo se puede consultar, por ejemplo, el capítulo sobre anillos de división del libro de N. Jacobson, *Structure of rings*.

§ 1. *Anillos de división*

Se dice que un anillo asociativo R es un anillo de división, si

a) R contiene un elemento unidad distinto de cero, que llamaremos 1, y

b) Todo elemento de R distinto de cero posee un inverso a la derecha. Es decir, para todo $a \neq 0$, $a \varepsilon R$, existe un elemento que designaremos por a^{-1}, $a^{-1} \varepsilon R$, tal que

$$aa^{-1} = 1.$$

Se comprueba inmediatamente que $a^{-1}a = 1$. Pues sea $(a^{-1})^{-1}$ el nverso de a^{-1}, entonces, se verifica

$$a = a \cdot 1 = a[a^{-1}(a^{-1})^{-1}] = (aa^{-1})\,(a^{-1})^{-1} = (a^{-1})^{-1}$$

y, por tanto,

$$a^{-1}a = 1.$$

La razón del nombre «anillo de división» aparecerá más claramente si adoptamos la siguiente definición que, según el lector podrá comprobar, es equivalente a la primera:

Un anillo asociativo R se dice que es un anillo de división si

i) contiene un elemento distinto de cero, y

ii) dados dos elementos cualesquiera $a, b \varepsilon R$, si $a \neq 0$, existen elementos $x, y \varepsilon R$ que safisfacen las ecuaciones

$$ax = b \quad , \quad ya = b.$$

Nótese que en esta definición no es necesario postular que R contiene un elemento unidad, sino que la existencia de un elemento unidad es una consecuencia de la definición. Si no impusiéramos la condición de que el anillo posee un elemento distinto de cero, el anillo que contiene únicamente el elemento cero resultaría un anillo de división y es conveniente no considerar tal anillo como anillo de división.

Cuando el anillo de división R es conmutativo se suele decir que R es un cuerpo; en caso de que R no sea conmutativo se emplea tambien la expresión: cuerpo no conmutativo. En el presente artículo usaremos el término cuerpo para designar un anillo de división conmutativo; cuerpo no conmutativo para indicar un anillo de división *no conmutativo* y cuando hablemos de un anillo de división entenderemos que puede ser conmutativo o no conmutativo.

Los ejemplos mas conocidos de cuerpos son el cuerpo de los números racionales, los números algebraicos, los numeros reales, los complejos y el cuerpo de números *p*-ádicos. Cada uno de estos cuerpos contiene un subcuerpo isomorfo al cuerpo de los numeros racionales Q, pero este último no contiene ningun subcuerpo propio, es decir, ningún subconjunto de Q, distinto de Q, forma un cuerpo. Quiza resulte conveniente recordar, que, cuando se habla de un anillo de división no se hace referencia simplemente al conjunto de sus elementos, sino a dicho conjunto con las correspondientes operaciones de suma y multiplicación definidaentre sus elementos.

Puesto que el cuerpo de los numeros racionales contiene un numero infinito de elementos, más exactamente, una infimidad numerable, todos los ejemplos arriba mencionados poseen una infinidad, numerable o no numerable, de elementos. Pero existen tambien cuerpos con un número finito de elementos; tales cuerpos reciben el nombre de cuerpos finitos o cuerpos de Galois. El ejemplo más sencillo de cuerpo con un número finito de elementos es el cuerpo conteniendo *p* elementos, donde *p* es un numero primo cualquiera; tal cuerpo F_p es isomorfo al conjunto de las clases de restos de los numeros enteros módulos *p*, con las definiciones ordinarias de suma y multiplicación. Todo cuerpo con un numero finito de elementos contiene un subcuerpo isomorfo a F_p y se demuestra fácilmente que el número de elementos de un cuerpo de Galois es la potencia de un número primo *p*. Inversamente, si $N = p^n$, *n* un entero positivo, existe un cuerpo que contiene exactamente N elementos y todos los cuerpos que contienen exactamente N elementos son isomorfos entre sí. En otros términos, un cuerpo de Galois está completamente definido salvo isomorfismo por su número de elementos.

§ 2. *Cuerpos no conmutivos*

El primer ejemplo de cuerpo no conmutivo fue construido hace unos cien años por el matematico irlandés Sir W. R. Hamilton. Este es el cuerpo no conmutativo de los cuaternios, que suponemos conocido por el lector. Recordemos simplemente que si R es el cuerpo de los números reales el cuerpo de los cuaternios esta constituído por el conjunto de elementos de la forma

$$a = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k,$$

donde $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \varepsilon R$ y i, j, k son tres elementos que conmutan con todos los elementos de R y cuya tabla de multiplicación está definida por las igualdades siguientes:

$$i^2 = j^2 = k^2 = -1 \; ; \; ij = -ji = k \; ; \; jk = -kj = i \; ; \; ki = -ik = j.$$

Si calculamos el producto de a y $\bar{a} = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$ obtenemos

$$a\bar{a} = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 = \beta = N(a)$$

y $N(a) = 0$ unicamente cuando $\alpha_0 = \alpha_1 = \alpha_2 = \alpha_3 = 0$, es decir, cuando $a = 0$. Por tanto si $a \neq 0$, $N(a) \neq 0$, $(N(a))^{-1}$ existe y $(N(a))^{-1}\bar{a} = a^{-1}$.

Podríamos intentar construir cuaternios sobre un cuerpo de Galois, pero nuestra construcción no puede conducirnos a un anillo de división, pues el numero de elementos distintos de la forma $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ que obtendríamos, suponiendo que los elementos α_i pertenecen a un cuerpo de Galois con $N = p^n$ elementos, seria p^{4n} y a principios de este siglo J. H. M. Wedderburn demostró que todo anillo de división con un número finito de elementos es necesariamente conmutativo (véase [8]). En otras palabras, si un anillo de división D posee sólo un número finito de elementos, D es un cuerpo de Galois.

Naturalmente el significado del teorema de Wedderburn es mas general que el hecho de que no podemos construir un cuerpo no conmutativo de cuaternios sobre un cuerpo de Galois. Existen generalizaciones del resultado de Wedderburn, esto es, teoremas que afirman que cuando un anillo de división satisface ciertas condiciones es un cuerpo; en particular estas condiciones son cumplidas por todos los anillos de división con un número finito de elementos.

Con el fin de describir algunos resultados de la teoría de cuerpos no conmutativos, necesitamos introducir algunas definiciones. Estas definiciones se pueden extender a un anillo asociativo cualquiera y, por ello, las presentamos en su forma más general.

Sea A un anillo asociativo cualquiera, el subconjunto C de elementos de A que conmutan con cada uno de los elementos de A recibe el nombre de centro de A. En símbolos.

$$C = \{ c / \quad ca = ac \quad , \quad a \varepsilon A \}$$

Se comprueba inmediatamente que C es un subanillo conmutativo y, en particular, si A es un anillo de división, su centro C contiene elé-

mentos distintos de cero, porque el elemento unidad pertenece al centro, y C es un cuerpo.

Si F es un anillo de división contenido en un anillo asociativo A, tomando como ley de composición de un elemento $f \varepsilon F$ con un elemento $a \varepsilon A$ el producto $fa \varepsilon A$, podemos considerar a A como espacio vectorial a la izquierda sobre F. Definimos la dimensión a la izquierda de A sobre F, $[A : F]_i$, como la dimensión de A considerado como espacio vectorial a la izquierda sobre F. Analogamente, A puede ser considerado como espacio vectorial a la derecha sobre F y definiremos $[A : F]_d$ como la dimensión de A como espacio vectorial a la derecha sobre F. Si F está contenido en el centro de A, la estructura de A como espacio vectorial a la izquierda sobre el cuerpo F es isomorfa a su estructura de espacio vectorial a la derecha. En particular si D es un cuerpo no conmutativo y C es su centro, llamaremos dimensión de D sobre su centro a $[D : C]_i = [D : C]_d$, que denotaremos simplemente por $[D : C]$. Cuando la dimensión $[D : C]$ es finita se dice que D es una extensión finita de C.

En el ejemplo de los cuaternios el centro es el conjunto de elementos de la forma $\alpha + oi + oj + ok$ que suelen representarse simplemente por α. El centro es, pues, isómorfo al cuerpo de los números reales y la dimensión del cuerpo no conmutativo de cuaternios sobre su centro es cuatro y de ahí su nombre.

En general, si E es un anillo de división contenido en el cuerpo no conmutativo D, necesitamos imponer ciertas condiciones para poder demostrar que $[D : E]_i = [D : E]_d$. Aunque todavía no ha sido publicado, parece ser que se ha construido un ejemplo de cuerpo no conmutativo D, conteniendo un anillo de división E tal que $[D : E]_i = 2$, pero $[D : E]_d = \infty$.

A principios de este siglo, L. E. Dickson indicó una forma de construir un anillo extensión finita de un cuerpo y dio un ejemplo en que el anillo así obtenido es un cuerpo no conmutativo. La no conmutatividad es una consecuencia de la construcción y Wedderburn estableció la condición necesaria y suficiente para que los anillos así construidos fuesen cuerpos no conmutativos. Estos resultados y las referencias a los artículos originales se pueden encontrar en [1] apéndice I.

Si b es un elemento de un anillo asociativo R con unidad y b posee un inverso en R, es decir, existe un elemento b^{-1} tal que $b^{-1}b = bb^{-1} = 1$, la transformación σ definida por

$$c^{\sigma} = b^{-1} cb$$

es un automorfismo de R. Si b no pertenece al centro de R, σ es un automorfismo distinto del automorfismo idéntico. Los automorfismos así definidos se llaman automorfismos interiores. Resulta claro que todo automorfismo interior deja invariantes los elementos del centro y que los automorfismos interiores forman un grupo.

Para los cuerpos no conmutativos D de dimensión finita sobre su centro se han demostrado los dos teoremas siguientes:

I) La dimensión de D sobre su centro C es un cuadrado. Esto es $[D : C] = n^2$.

II) Todo automorfismo de D que deja invariantes los elementos del centro es un automorfismo interior.

Pasemos ahora a considerar cuerpos no conmutativos de dimensión infinita sobre su centro. Un ejemplo de cuerpo no conmutativo con esta propiedad fue dado por D. Hilbert en [2], § 33. En dicho ejemplo todo elemento del cuerpo no conmutativo D que no pertenece al centro C, es un elemento transcendente sobre C. En otras palabras, los elementos que no pertenecen al centro no anulan ningun polinomio con coeficientes en C. En 1931, G. Koethe publicó un artículo, [4], conteniendo ejemplos de cuerpos no conmutativos E de dimensión infinita sobre su centro C, en que todo elemento de E anula un cierto polinomio con coeficientes en C. Expresado en otra forma, el cuerpo no conmutativo E es algebraico sobre su centro.

No resulta difícil construir cuerpos no conmutativos de dimensión infinita sobre su centro C y conteniendo elementos algebraicos α, $\alpha \varepsilon / C$ y elementos transcendentes sobre C. Para la construcción de ejemplos de cuerpos no conmutativos son muy utiles los resultados de O. Ore en relación con el siguiente problema:

¿Es posible sumergir un anillo asociativo R sin divisores de cero en un anillo de división?:

Cuando R es asociativo siempre es posible sumergirlo en un cuerpo mínimo. Tal cuerpo consiste solamente de los elementos de R y los «cocientes» de dichos elementos. Si R es no conmutativo tendremos que distinguir entre el cociente a la derecha x de b dividido por c, esto es, $b = cx$ y el cociente a la izquierda y, $b = yc$. Si R es un anillo no conmutativo sin divisores de cero diremos que el cuerpo no conmutativo D, es un cuerpo de cocientes a la izquierda respecto de R, si todo elemento x de D es de la forma ba^{-1}, b, $a \varepsilon R$, o lo que es lo mismo $b = xa$. El cuerpo de cocientes a la derecha se define analogamente, siendo ahora

$$x = a^{-1}b, \quad a, \quad b \varepsilon R.$$

Ore demostró en [6] que un anillo asociativo sin divisores de cero posee un cuerpo de cocientes a la izquierda cuando, y sólo cuando, dos elementos cualesquiera $a, b \varepsilon R$ poseen un multiplo común a la derecha, es decir, $ab_1 = ba_1$, donde b_1, $a, \varepsilon R$. Existe un resultado dual intercambiando los términos derecha e izquierda. En este mismo artículo se halla un ejemplo de un anillo especial sin divisores de cero, en el cual no es cierto que dos elementos cualesquiera poseen un múltiplo común a la derecha o a la izquierda, sin embargo, dicho anillo esta contenido en un cuerpo no conmutativo, el cual, naturalmente, no es un cuerpo de cocientes. El anillo es especial porque sólo cumple la ley distributiva a la derecha $(a + b)c = ac + bc$, pero, en general, $c(a + b) \neq ca + cb$.

En [7], Ore estudia construcciones de anillos asociativos no conmutativos, sin divisores de cero ,en los cuales dos elementos cualesquiera poseen un múltiplo común a la izquierda y, por tanto, pueden ser su-

mergidos en un cuerpo de cocientes a la derecha. Sin embargo, en [8], A. Malcev demostró mediante un ingenioso ejemplo que no todo anillo asociativo sin divisiones de cero puede ser sumergido en un anillo de división.

BIBLIOGRAFIA

[1] DICKSON, L. E.: *Algebras and their arithmetics*, 1923. Reeditado por Dover Publications, 1960.

[2] HILBERT, D.: *Grundlagen der Geometrie.* Existe traducción española publicada por el C. S. I. C.

[3] JACOBSON, N.: «Structure of rings». *Am. Math. Soc.* Colloqium Publications, vol. 37, 1956.

[4] KOETHE, G.: «Schiefkorper unendlichen Ranges uber dem Zentrum», *Math. Ann.*, vol. 105 (1931), págs. 15-39.

[5] MALCEV, A.: «On the inmersion of an algebraic ring into a field». *Math. Ann.*, vol. 113 (1936), págs. 686-91.

[6] ORE, O.: «Linear equations in non-conmutative fields». *Ann. of Math.*, vol. 32 (1931), págs. 463-77.

[7] ORE, O.: «Theory of non-conmutative polynomials». *Ann. of Math.*, vol. 34 (1933), págs. 480-508.

[8] WEDDERBURN, J. H. M.: «A theorem on finite algebras». *Trans. Amer. Math. Soc.*, vol 6 (1905), pags. 349-352.