# NUMEROS COMPLEJOS Y GENERALIZACIONES

Enzo R. Gentile

*El objeto de este trabajo es dar una fundamentación natural de la definición de Número Complejo. El problema principal, como es bien sabido, es tratar de resolver la ecuación* $X^2 + 1 = 0$ *, carente de solución en el cuerpo de los números reales. Resolver la ecuación significa extender el cuerpo real a un cuerpo que contenga un elemento* $\mathfrak{L}$ *que satisfaga la ecuación* $\mathfrak{L}^2 + 1 = 0$ *o equivalentemente* $\mathfrak{L}^2 = -1$ *. Este problema no es otra cosa que un caso particular del siguiente problema general: dado un cuerpo* k *y un polinomio* p(X) *con coeficientes en* k *e irreductible sobre* k *se pide construir un cuerpo* A *, extensión de* k *, que contenga un elemento* $\mathfrak{L}$ *que sea raíz de* p(X)*, o sea* $p(\mathfrak{L}) = 0$ *.*

*Por supuesto que esta es tarea habitual en los cursos de Algebra II ó III, sin embargo es nuestra pretensión al escribir estas Notas mostrar que por el mismo precio, la fundamentación natural del problema sobre los números complejos permite resolver el problema general. O sea, pretendemos señalar el carácter elemental de estas construcciones y es nuestra esperanza que estas ideas puedan incorporarse a cursos elementales de Algebra.*

## 1. Introducción

Los números complejos suelen introducirse sistemáticamente como pares ordenados de *números reales* (x, y) con las operaciones de

(D)

$$\textit{suma:} \qquad (x,y) + (x',y') = (x+x',\ y+y')$$

$$\textit{producto:} \qquad (x,y)\ .\ (x',y') = (xx' - yy',\ xy' + x'y)$$

La definición de suma es "natural". No es así con el producto. Ciertamente ningún alumno curioso puede aceptar gratuitamente esa definición de producto. Sin embargo, en los cursos de álgebra o análisis, al introducir de esta forma los complejos, raramente alguien pregunta el motivo de esa definición. Veamos entonces primeramente cuál puede ser una motivación razonable de la definición (D).

Un problema fundamental clásico lo constituye la resolución de las ecuaciones algebraicas

$$a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 = 0 \quad , \quad a_n \neq 0$$

donde $a_n, \ldots, a_0$ son coeficientes numéricos y se trata de hallar un "número" digamos x que satisfaga la ecuación anterior, o sea tal que

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0 .$$

Por ejemplo si la ecuación es de primer grado: $a_1 X + a_0 = 0$ y los $a_i$ son elementos de Q ó de R, la ecuación tiene única solución $x = -a_0 . a_1^{-1}$ .

En el caso de la ecuación de segundo grado, escribamos como es habitual,

(1) $$aX^2 + bX + c = 0 \quad , \quad a \neq 0 \quad , \quad a,b,c \text{ en } Q \text{ ó en } R .$$

Completando cuadrados resulta

$$a\left(X + \frac{b}{2a}\right)^2 - \frac{b^2}{4a} + c = 0$$

o sea

$$a\left(X + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a}$$

(2) $$\left(X + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}$$

De aquí se sigue inmediatamente que la ecuación de segundo grado es resoluble (en Q ó en R) sí y sólo si $b^2 - 4ac$ es un cuadrado.

En efecto, escribimos

$$b^2 - 4ac = t^2$$

y entonces

$$(X + \frac{b}{2a})^2 = (\frac{t}{2a})^2 \quad \text{es decir} \quad X + \frac{b}{2a} = \pm \frac{t}{2a} .$$

Por lo tanto, $X = -\frac{b}{2a} \pm \frac{t}{2a} = \frac{-b \pm t}{2a}$

y esta es la clásica fórmula general de resolución por radicales, de la ecuación de segundo grado. En general, trabajando en el cuerpo de números racionales un gran número de elementos no son cuadrados, de manera que la resolución de la ecuación de segundo grado puede no ser posible. En el caso real sabemos bien que "un número real r es un cuadrado *si* y sólo si $r \geq 0$".

Entonces si $b^2 - 4ac$ es un cuadrado en R, la ecuación (1) es resoluble. O equivalentemente, cuando $b^2 - 4ac \geq 0$ . En la situación $b^2 - 4ac < 0$ podemos escribir (2)

$$(X + \frac{b}{2a})^2 = -1 . (\frac{4ac - b^2}{4a^2}) = -1 . (\frac{t}{2a})^2$$

con $t^2 = 4ac - b^2 > 0$ .

Se sigue de esta discusión la siguiente observación fundamental: *Las ecuaciones cuadráticas con coeficientes reales son todas resolubles si podemos sumergir a* R *en un cuerpo donde* -1 *sea un cuadrado.*

Nuestra primer tarea será *sumergir* a R en un anillo conmutativo donde -1 sea un cuadrado, o sea, simbólicamente, encontrar un anillo conmutativo K que contenga a R y donde exista un elemento £ tal que $£^2 = -1$. Por supuesto que en pedir que exista un anillo conmutativo K que contenga a R entendemos que las operaciones de anillo de K restringidas a R coinciden con las operaciones de anillo de R (o sea R *es un subanillo de* K). Podemos debilitar la condición de que K sea un anillo conmutativo pidiendo que R esté sumergido en un anillo K (no necesariamente conmutativo) pero donde exista un elemento £ tal que satisfaga las dos condiciones siguientes:

$$\mathfrak{L}^2 = -1 \quad y \cdot \forall r \in R \ , \ r.\mathfrak{L} = \mathfrak{L}.r$$

Para el lector inquieto conocedor del anillo de matrices le podemos mostrar un ejemplo transparente de esta inmersión. A saber, sea K el anillo de matrices de 2x2 con coeficientes reales. La inmersión natural de R en K esta dada por

$$r \longrightarrow \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix}$$

y el elemento $\mathfrak{L}$ que buscamos es (por ejemplo):

$$\mathfrak{L} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

Por ahora no nos interesa conocer la existencia efectiva de un "habitat" para R. La idea es suponer la existencia del anillo K y deducir la posible estructura de un anillo que extienda a R y contenga el elemento $\mathfrak{L}$ .

Es claro que un anillo K al contener a R y al elemento $\mathfrak{L}$ debe contener todas las combinaciones de estos *vía* el producto y la suma, por ejemplo debe contener

$$\mathfrak{L} \ , \ \mathfrak{L}^2, \ \mathfrak{L}^3, \ldots$$

$$r_1\mathfrak{L} \ , \ r_2\mathfrak{L}^2 \ , \ r_3\mathfrak{L}^3 \ , \ldots \qquad r_i \in R$$

y en general a expresiones polinomiales

$$\boxed{r_0 + r_1\mathfrak{L} + r_2\mathfrak{L}^2 + \ldots + r_n\mathfrak{L}^n \ , \ r_i \in R}$$

La totalidad de tales expresiones polinomiales es un anillo conmutativo que denotamos por A (en este punto es necesaria la hipótesis que $r.\mathfrak{L} = \mathfrak{L}.r$ , si $r \in R$).

Se tienen entonces las inclusiones $R \subset A \subset K$ . El anillo A contiene a $\mathfrak{L}$ , es por lo tanto suficiente limitarnos a trabajar en el

anillo A. No nos interesa en este momento saber si A es un cuerpo. Queremos conocer un poco más de la naturaleza de los elementos de A. Hagamos, a tal fin, la siguiente observación: las potencias $\mathfrak{L}^j$ cuando j recorre los números naturales *no* son todas distintas entre sí:

$$\mathfrak{L}^2 = -1 \ , \ \mathfrak{L}^3 = -\mathfrak{L} \ , \ \mathfrak{L}^4 = 1 \ , \ \mathfrak{L}^5 = \mathfrak{L} \ , \ldots$$

o sea hay periodicidad módulo 4. Se sigue que la forma más general es ahora

$$a + b.\mathfrak{L} \quad \text{con} \quad a,b \in R \ .$$

Pero algo más. Tal escritura es *única*: sea en efecto,

$$a + b.\mathfrak{L} = c + d.\mathfrak{L} \quad \text{en } A \ , \ a,b,c,d \ \text{en} \ R$$

Si $a = c$ entonces $b.\mathfrak{L} = d.\mathfrak{L}$ y multiplicando por $\mathfrak{L}$ resulta $-b = -d$ , o sea $b=d$. Por lo tanto la unicidad. Si $a \neq c = (d-b).\mathfrak{L}$. Se sigue que $d-b \neq 0$ y siendo $d-b \in R$ se concluye que

$$\mathfrak{L} = \frac{a-c}{d-b} \in R \ ,$$

*un absurdo*. Se sigue la unicidad afirmada anteriormente. En conclusión, dentro de K hemos encontrado un anillo A, que contiene a R y al elemento $\mathfrak{L}$ . Sus elementos se escriben unívocamente en la forma $a + b.\mathfrak{L}$ , a y b en R. Notar que esto confiere a A cierto viso de unicidad. No costaría nada probar que A es además un cuerpo. Nos contentamos con haber encontrado un anillo, extensión de R donde -1 es un cuadrado. La suma y producto en A no son otra que operar con polinomios.

Veamos: $(a+b.\mathfrak{L}) + (c+d.\mathfrak{L}) = (a+c) + (b+d).\mathfrak{L}$

$$(a+b.\mathfrak{L}).(c+d.\mathfrak{L}) = ac + ad.\mathfrak{L} + b.\mathfrak{L}.c + b.\mathfrak{L}.d.\mathfrak{L}$$

y utilizando la propiedad asociativa y conmutativa resulta,

$$= ac + ad.\mathfrak{L} + bc.\mathfrak{L} + bd.\mathfrak{L}^2$$

$$= (ac-bd) + (ad+bc).\mathfrak{L}$$

y en algún sentido observamos que hemos recuperado las operaciones primitivas (D).

*Epílogo:* Si "los complejos" existen, su definición tiene que estar dada por las relaciones que acabamos de encontrar. Por lo tanto el próximo paso es sacar de esta discusión las ideas fundamentales. Por ejemplo, los elementos de A estan representados *unívocamente* por binomios $a + b.\pounds$ . Por lo tanto definiremos un conjunto de pares ordenados de números reales, o sea consideraremos el conjunto $C = R \times R$. Las operaciones de suma y producto se harán a la manera de lo que acabamos de hacer. Estas son las clásicas fórmulas de suma y producto (D). Todo el trabajo se reduce a ver que estas definiciones "funcionan". Pero este trabajo es simple. Esperamos que ahora sí el lector se sienta motivado y acepte las definiciones de suma y producto y algo más, ¡con tranquilidad!.

El tratamiento que sigue es ahora formal. Por supuesto que al elemento £ lo indicaremos como es usual utilizando la notación de Euler (1707-1783) $\pounds = i$: llamada *unidad imaginaria*. Las denominaciones de Números Complejos es debida originalmente a Descartes (1596-1650) y adoptada por C.F. Gauss (1777-1855).

## 2. Números Complejos

*Def.:* Sea $C = R \times R = \{(a,b)/a,b \in R\}$ = Pares ordenados de Números Reales.

$= : (a,b) = (a', b')$ sí y sólo sí $a = a'$ y $b = b'$

(+): *suma*: $(a,b)+(c,d) = (a+c, b+d)$

(.): *producto*: $(a,b).(c,d) = (ac-bd, ad+bc)$

*Proposición:* **C** dotado de suma (+) y producto (.) es un anillo conmutativo con

$(0,0)$ por elemento neutro de la suma

$(1,0)$ por elemento neutro del producto.

*Dem.:* Ejercicio.

Notemos que todo elemento $(a,b)$ en **C** puede escribirse en la forma

$$(a,b) = (a,0) + (0,b)$$

Los elementos de $\mathbf{C}$ con segunda componente nula, o sea los elementos $(a,0)$ satisfacen las propiedades

$$(a,0) + (a',0) = (a+a',0)$$
$$(a,0) \cdot (a',0) = (aa',0)$$
$$(1,0) \cdot (a,0) = (a\ ,\ 0)$$

de manera que si definimos la aplicación

$$R \longrightarrow \mathbf{C}$$
$$a \longrightarrow (a,0)$$

R *se identifica a los pares en* $\mathbf{C}$ *con segunda componente* 0 .

Entonces si $a \in R$

$$a.(b,c) = (a,0).(b,c) = (ab,ac)$$
$$a.(0,1) = (0,\ a)$$

Además $(a,b) = (a,0) + (0,b) = a.(1,0) + b.(0,1) =$

$$= a.1 + b.(0,1)$$

Por lo tanto si llamamos, como es habitual,

$$i = (0,1)$$

se tiene

$$\boxed{(a,b) = a + b.i} \qquad a,b \text{ en } R$$

*En resumen*, los elementos de $\mathbf{C}$ se representan en la forma

$$a + b.i \quad \text{con} \quad a,b \quad \text{en} \quad R$$

Además $a + b.i = a' + b'.i$ sí y sólo sí $a = a'$ y $b = b'$

$$(a + b.i) + (a' + b'.i) = (a + a') + (b + b').i$$

$$(a + b.i) \cdot (a' + b'.i) = (aa' - bb') + (ab' + ba').i$$

$$i^2 = -1$$

Sea $a + b.i \neq 0 = 0 + 0.i$, por lo tanto $a \neq 0$ ó $b \neq 0$. Por lo tanto, en R!

$$a^2 + b^2 \neq 0 \ .$$

Se sigue entonces que

$$(a+b.i).\left(\frac{a}{a^2+b^2}+\frac{-b}{a^2+b^2}.i\right)=\frac{1}{a^2+b^2}.(a^2+b^2)=1$$

o sea $(a+b.i)$ es inversible en **C**. Hemos probado entonces que **C** dotado de suma y producto como indicamos más arriba, es un cuerpo: el *Cuerpo de los Números Complejos*, o *Cuerpo Complejo*.

## 3. Digresión para conocedores de matrices

La discusión inicial referente a la definición de números complejos sugiere una realización de los mismos como un tipo particular de matrices reales de 2x2. Sea, en efecto, $M_2(R)$ la totalidad de matrices

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \quad , \quad a_{ij} \in R$$

con suma y productos ordinarios. $M_2(R)$ es un anillo con elemento neutro la matriz identidad

$$I=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Los números reales admiten, en forma natural, una representación dentro de $M_2(R)$ a saber

$$r \in R \longrightarrow \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} \qquad (1)$$

Esta representación permite *identificar* a R con la totalidad de matrices del tipo (1) denominadas *escalares*. Dentro de $M_2(R)$ vive la matriz

$$\mathfrak{L}=\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

que satisface:

$$\mathcal{L}^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -1$$ (poniendo en función la identificación precedente)

y verifica: $r.\mathcal{L} = \mathcal{L}.r$, $\forall r \in R$.

Podemos analizar la discusión inicial en este nuevo contexto para descrubir dentro de $M_2(R)$ un anillo cuyos elementos son de la forma

$$a + b.\mathcal{L} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} + \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} + \begin{bmatrix} 0 & -b \\ b & 0 \end{bmatrix} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \quad (2)$$

Esta es la realización buscada!: los complejos se identifican a las matrices reales de 2x2 del tipo (2). La correspondencia es:

$$a + b.i \longrightarrow \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

4. Generalización 1

La discusión precedente no utiliza ninguna propiedad relevante del cuerpo R en cuanto se refiere a la construcción del anillo A de expresiones polinomiales

$$a + b.\mathcal{L} \quad , \quad a \text{ y } b \text{ en } R$$

La propiedad del cuerpo real que se utiliza es que, en R: "$a^2 + b^2 = 0$ si y sólo si $a = b = 0$". De aquí se sigue que A es un cuerpo.

Sea en general k un cuerpo conmutativo. Podemos construir un anillo A que contiene a k y contiene un elemento $\mathcal{L}$, $\mathcal{L} \notin k$ tal que $\mathcal{L}^2 = -1$. La construcción es simplemente la dada por los pares

$$a + b.\mathcal{L} \quad , \quad a, b \in k \quad , \quad \mathcal{L}^2 = -1$$

como hicimos anteriormente. La cuestión pertinente es ahora determi

nar en que condiciones *sobre* k es el anillo A un cuerpo. En caso afirmativo habremos sumergido a k en un cuerpo A que resuelve la ecuación $X^2 + 1 = 0$.

La forma de resolver este problema se logra considerando la expresión cuadrática

$$N(a+b.\pounds) = (a+b.\pounds),(a-b.\pounds) = a^2 + b^2$$

llamada la *norma* del elemento $a+b.\pounds$ de A. Es un ejercicio sencillo probar que la norma es una función multiplicativa: $N(x.y) = N(x).N(y)$. Además $N(1) = 1$. Entonces afirmamos que un elemento $a+b.\pounds \in A$ es inversible si y sólo si $N(a+b.\pounds) \neq 0$. En efecto, si $(a+b.\pounds).(c+d.\pounds) = 1$ (o sea $a+b.\pounds$ es inversible) entonces

$$1 = N(a+b.\pounds).N(c+d.\pounds)$$

con lo que $N(a+b.\pounds) \neq 0$.

Recíprocamente si $N(a+b.\pounds) = a^2 + b^2 \neq 0$, entonces el elemento $\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}.\pounds$ es inverso de $a+b.\pounds$. La afirmación queda probada.

Se sigue como corolario fundamental que: A es un cuerpo si y sólo si se satisface en k la siguiente propiedad:

$$a^2 + b^2 = 0 \rightarrow a = b = 0$$

Podemos dar ejemplos de cuerpos con esta propiedad

i. $k = Z_3$ el cuerpo de restos módulo 3

ii. $k = Z_7$ el cuerpo de restos módulo 7

iii. $k = Q$ el cuerpo racional

Ejemplos que no satisfacen esta propiedad

i. $k = Z_2$ el cuerpo de restos módulo 2 $(1^2 + 1^2 = 0)$

ii. $k = Z_5$ el cuerpo de restos módulo 5 $(1^2 + 2^2 = 0)$

iii. $k = \mathbb{C}$ el cuerpo complejo $(1^2 + i^2 = 0)$

Notación: $k(i) = A$

Entonces $Z_3(i)$ es un cuerpo de 9 elementos. Una tabla de multiplicación en $Z_3(i)$ es la siguiente:

| | 0 | 1 | 2 | i | 2i | 1+i | 1+2i | 2+i | 2+2i |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | i | 2i | 1+i | 1+2i | 2+i | 2+2i |
| 2 | 0 | 2 | 1 | 2i | i | 2+2i | 2+i | 1+2i | 1+i |
| i | 0 | i | 2i | 2 | 1 | 2+i | 1+i | 2+2i | 1+2i |
| 2i | 0 | 2i | i | 1 | 2 | 1+2i | 2+2i | 1+i | 2+i |
| 1+i | 0 | 1+i | 2+2i | 2+i | 1+2i | 2i | 2 | 1 | i |
| 1+2i | 0 | 1+2i | 2+i | 1+i | 2+2i | 2 | i | 2i | 1 |
| 2+i | 0 | 2+i | 1+2i | 2+2i | 1+i | 1 | 2i | i | 2 |
| 2+2i | 0 | 2+2i | 1+i | 1+i | 2+i | i | 1 | 2 | 2i |

Al igual $Z_7(i)$ es un cuerpo de $49 = 7^2$ elementos. Dejamos a cargo del lector calcular una tabla de multiplicación para este cuerpo.

La pregunta natural que uno se formula entonces es: *¿Para que primos* p *es* $Z_p(i)$ *un cuerpo?*

La respuesta está dada en el siguiente teorema:

Teorema: Sea p un primo positivo impar. Las condiciones siguientes son todas equivalentes entre sí:

i. p no es suma de dos cuadrados

ii. $Z_p(i)$ es un cuerpo

iii. $X^2 \equiv -1 \pmod p$ no admite solución en Z (o sea -1 no es residuo cuadrático módulo p)

iv. Existe $m \in Z$ tal que $p = 4m + 3$

v. $p \mid a^2 + b^2$ en $Z \Rightarrow p \mid a$ y $p \mid b$

La demostración de este teorema la omitiremos aquí, puede consultarse en cualquier libro de Teoría Elemental de Números o también en un artículo próximo sobre Divisibilidad en esta Revista.

5. Generalización 2

La construcción original de $\mathbf{C}$ que efectuamos en la primera parte de este artículo podemos ahora generalizarla si abandonamos el polinomio $X^2 + 1$, o equivalentemente la ecuación $X^2 + 1 = 0$. Hay razones para ello. En efecto, sobre el cuerpo Q no es posible resolver, por ejemplo, la ecuación $X^2 - 2 = 0$, dado que el número real $\sqrt{2}$ que resuelve esta ecuación no es racional. En nuestra discusión deberemos entonces reemplazar la condición $\mathfrak{L}^2 = -1$, por $\mathfrak{L}^2 = 2$, si tratamos de extender Q de manera tal de resolver la ecuación $X^2 - 2 = 0$. Obtendremos un anillo A cuyos elementos tienen la representación $a + b.\mathfrak{L}$, $a,b \in Q$, $\mathfrak{L}^2 = 2$ y las operaciones son

$$(a+b.\mathfrak{L}) + (c+d.\mathfrak{L}) = (a+c) + (b+d).\mathfrak{L}$$
$$(a+b.\mathfrak{L}) \cdot (c+d.\mathfrak{L}) = (ac+2db) + (ad+bc).\mathfrak{L}$$

Si $a+b.\mathfrak{L} \in A$ y $a \neq 0$ ó $b \neq 0$ entonces $a^2 - 2.b^2 \neq 0$ pues $X^2 - 2 = 0$ carece de solución en Q. Por lo tanto

$$(a + b.\mathfrak{L}) \cdot \left(\frac{a}{a^2-2.b^2} + \frac{-b}{a^2+2.b^2} \cdot \mathfrak{L}\right) = 1$$

de manera que A es un cuerpo. Lo denotamos con $Q(\sqrt{2})$ y en lugar de $\mathfrak{L}$ usamos $\sqrt{2}$ de manera que los elementos de A se escriben en la forma unívoca $a+b.\sqrt{2}$, $a, b \in Q$.

Por supuesto que en el caso de Q tenemos un "habitat" natural que es el cuerpo R de números reales o también el cuerpo $\mathbf{C}$ de números complejos.

Esta generalización la podemos aplicar al cuerpo $k = Z_5$ para construir un cuerpo de $25 = 5^2$ elementos. En efecto, la ecuación $X^2 - 2 = 0$ no admite solución en $Z_5$, dado que los cuadrados en $Z_5$ son 0,1,4. Repitiendo la construcción obtenemos un cuerpo denotado por $Z_5(\sqrt{2})$ cuyos elementos son las expresiones $a+b.\mathfrak{L}$ con a y b en $Z_5$, $\mathfrak{L}^2 = 2$.

*Factor:* construya una tabla de multiplicación en $Z_5(\sqrt{2})$!.

El caso de $Z_2$ también tiene una solución. Un polinomio sobre $Z_2$ que no admite ninguna raíz en $Z_2$ es $X^2 + X + 1$. Por lo tanto hay que repetir la construcción primitiva pero ahora £ debe satisfacer la ecuación $£^2 = £ + 1$. Se obtiene un cuerpo de 4 elementos cuya tabla de multiplicación es:

| . | 0 | 1 | £ | 1+£ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | £ | 1+£ |
| £ | 0 | £ | 1+£ | 1 |
| 1+£ | 0 | 1+£ | 1 | £ |

3. Generalización 3

Esta generalización consiste en abandonar el grado 2 que usamos en los polinomios para buscarles raíces. Por ejemplo podemos tomar $k = Q$ el cuerpo racional y buscar una solución de la ecuación $X^3 - 2 = 0$. Entonces el análisis del procedimiento nos revela que las expresiones polinomiales serán ahora del tipo

$$r_0 + r_1£ + r_2£^2 \quad , \quad r_i \in Q$$

y el producto debe hacerse reduciendo según la ecuación $£^3 = 2$. Es claro que se obtiene un anillo conmutativo A. No es tan inmediato ver que A es un cuerpo. Pero lo es !. Se trata de probar que si $z = r_0 + r_1£ + r_2£^2 \neq 0$ (o sea $(r_0, r_1, r_2) \neq (0, 0, 0)$ entonces z admite un inverso en A. Trabajemos con polinomios sobre $Q[X]$. El elemento z da lugar al polinomio de grado $\leq 2$, $r_2X^2 + r_1X + r_0$. Puesto que $X^3 - 2$ es irreductible sobre $Q[X]$, el máximo común divisor de ambos polinomios es 1 y podemos escribir

$$(r_2X^2 + r_1X + r_0).q(X) + (X^3-2).t(X) = 1$$

para polinomios $q(X), t(X) \in Q[X]$ convenientes.

Especializando el valor de X en £ , se sigue que $(r_2£^2 + r_1£ + r_0).q(£) = 1$ en A. Esto demuestra que A es un

cuerpo. Es bien claro que la propiedad esencial a pedir al polinomio de partida (como lo fue $X^3 - 2$) es la de ser irreductible.

*En general:* si k es un cuerpo y p(X) un polinomio *mónico*: $p(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ con coeficientes en k, podemos construir un anillo A de expresiones polinomiales

$$r_0 + r_1\mathfrak{L} + r_2\mathfrak{L}^2 + \ldots + r_{n-1}\mathfrak{L}^{n-1} \quad , \quad r_i \in k \ , \ \forall i$$

donde se onera con la regla que

$$\mathfrak{L}^n = - r_{n-1}\mathfrak{L}^{n-1} - \ldots - r_0$$

La propiedad de ser p(X) irreductible sobre k implica de inmediato que el anillo A es un cuerpo (la misma demostración precedente).

Siguiendo la idea de usar el anillo de matrices como hicimos al principio hay una forma de darle naturalidad a nuestra construcción. Sea $M = M_n(k)$ el anillo de matrices de $n \times n$. Al polinomio $p(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ le asociamos la matriz $C(p(X))$ llamada *"matriz compañera de* p(X)".

$$\begin{bmatrix} 0 & 0 & \cdot & \cdot & \cdot & -a_0 \\ 1 & 0 & \cdot & \cdot & \cdot & -a_1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 0 & -a_{n-2} \\ 0 & 0 & \cdot & \cdot & 1 & -a_{n-1} \end{bmatrix}$$

Por ejemplo

$$C(X-1) = [1] \quad , \quad C(X+1) = [-1]$$

$$C(X^2+1) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad , \quad C(X^2+X\ 1) = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$$

$$C(X^3-2) = \begin{bmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

Un ejercicio elemental en teoría de matrices nos muestra que la matriz $C(p(X))$ satisface la ecuación

$$p(C(p(X))) = 0$$

o sea la matriz $C(p(X))$ es *"raíz"* de $p(X)$ o también $p(X)$ *anula a* $C(p(X))$. Lo importante es para nosotros que en nuestra inmersión de k en un anillo, el anillo M es un gran candidato y precisamente $C(p(X))$ es el elemento $\mathfrak{L}$.

Estamos en condiciones de situarnos en un contexto completamente general de extensiones. Dado un cuerpo k, lo pensaremos sumergido en el anillo $M_n(k)$ de matrices, para todos los valores de n. Dado un polinomio irreductible $p(X) \in k[X]$ mónico y de grado n construímos dentro de $M_n(k)$ un cuerpo A generado por k y por una raíz de $p(X)$ dentro de $M_n(k)$. La raíz es precisamente la matriz compañera de $p(X)$. Este cuerpo consiste de todas las expresiones polinomiales de $C(p(X))$ con coeficientes en k. Lo interesante de esta construcción es que esta extensión de k está realizada por un conjunto de matrices. Por ejemplo en el caso original de los complejos la realización de **C** es la totalidad de matrices de $M_2(R)$ del tipo

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

Si consideramos el polinomio $X^3-2$ sobre Q se obtiene dentro de $M_3(Q)$ el cuerpo formado por todas las matrices del tipo $a + b.C(X^3-2) + c.(C(X^3-2))^2$ o sea

$$\begin{bmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{bmatrix} + b. \begin{bmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} + c. \begin{bmatrix} 0 & 2 & 0 \\ 0 & 0 & 2 \\ 1 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{bmatrix}$$

donde a,b y c recorren la totalidad de Q.

Las posibilidades de efectuar extensiones de este tipo a partir del cuerpo Q de números racionales son infinitas. En efecto, para cada n existen infinitos polinomios irreductibles (y además, coprimos de a dos) de grado n. Por ejemplo si p denota un número primo, para todo n natural el polinomio $X^n-p$ es irreductible sobre Q. En este caso la extensión produce una raíz n-sima de p.

Si p(X) es un polinomio irreductible sobre k y $\alpha$ es una raíz en alguna extensión de k como acabamos de ver, denotamos la extensión por $k(\alpha)$. Si p(X) tiene grado n entonces $k(\alpha)$ consiste de la totalidad de combinaciones lineales de las potencias $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ de $\alpha$ con coeficientes en k. Es fácil ver que $k(\alpha)$ es un espacio vectorial sobre k de dimensión n(= grado de p(X)). Es posible demostrar que esta extensión $k(\alpha)$ es única, salvo isomorfismos, o sea que la construcción que hemos efectuado *no depende del elemento* $\alpha$ que elegimos para efectuar la extensión.

Digamos que esto es sólo el principio de una parte importante del Algebra que es la teoría de cuerpos y que conduce a la teoría de ecuaciones algebraicas y a la teoría de Galois. Lo interesante sería que el lector que no tiene mucho entrenamiento en Algebra formal gastara algunos pensamientos en el tipo de construcción que hemos descripto y experimentara con algunos ejemplos, particularmente con cuerpos $Z_p$, matrices, etc. Que lo que hemos hecho es realmente importante para prestarle alguna atención se basa en que *todas* las extensiones finitas de k se logran por este método.

Como corolario se sigue que todas las extensiones de un cuerpo k de grado n están contenidas en $M_n(k)$. En un próximo artículo utilizaremos estas construcciones para referirnos al problema geométrico de construcciones con regla y compás.

Universidad de Buenos Aires.