El cuerpo de los números complejos como cuerpo de ruptura

El cuerpo algebraicamente cerrado de los números complejos es una extensión del cuerpo de los números reales, cuerpo al que estrictamente contiene como parte isomorfa. Se verifica en este campo de números el Teorema Fundamental del Algebra que establece que todo polinomio de *R[x]* de grado *n* tiene exactamente *n* raíces complejas. Constituyen los números complejos la principal herramienta matemática de desarrollo para múltiples áreas, tanto de la matemática como de la física (ecuaciones diferenciales, variable compleja, electromagnetismo, mecánica cuántica, etc.). Su exitosa representación geométrica como puntos de un plano (se trata de pares de números reales), permite su estudio elemental.

A continuación describimos la estructura de cuerpo conmutativo para el conjunto de todos los números complejos y veremos que puede generarse algebraicamente como extensión algebraica del cuerpo de los números reales, siendo isomorfo al cuerpo de ruptura del espacio cociente $R[x]/(x^2+1)$.

El cuerpo de los números complejos

Definiciones básicas:
Un *número complejo* es un par ordenado de números reales. El primero se denomina *parte real*, y el segundo *parte imaginaria*.

$$a=(x,y)\rightarrow\begin{cases} x=\text{parte real de}(a) \\ y=\text{parte imag de}(a)\end{cases}$$

Llamaremos C al conjunto de todos los números complejos.

Criterio de igualdad de números complejos
Dos números complejos $z_1=(x_1,y_1)$ y $z_2=(x_2,y_2)$ se dicen *iguales* si los pares correspondientes son iguales, esto es, si son iguales sus partes reales y también son iguales sus partes imaginarias.

$$z_1=z_2\leftrightarrow\begin{cases} x_1=x_2 \\ y_1=y_2\end{cases}$$

Suma y producto

a) Suma:

Se define la *suma* de dos números complejos como otro número complejo cuya parte real es la suma de las partes reales y cuya parte imaginaria es la suma de las partes imaginarias.

$$z_1+z_2=(x_1,y_1)+(x_2,y_2)=(x_1+x_2,y_1+y_2)$$

b) Producto:

Se define el *producto* de dos números complejos como otro número complejo cuya parte real se obtiene como la diferencia entre el producto de las partes reales y el producto de las partes imaginarias, mientras que la parte imaginaria se obtiene como la suma de los productos cruzados (parte imaginaria de uno por la parte real del otro).

$$z_1.z_2=(x_1,y_1).(x_2,y_2)=\left(x_1.x_2-y_1.y_2,x_1y_2+x_2y_1\right)$$

La estructura de cuerpo conmutativo

Definidas las anteriores operaciones de suma y producto, podemos comprobar que las propiedades que se deducen de las mismas confieren a todo el conjunto de estos números estructura de *cuerpo conmutativo*.

- Estructura de *C* como grupo aditivo conmutativo $(C,+)$:

Propiedad asociativa:

$$z_1+(z_2+z_3)=(x_1,y_1)+\left[(x_2,y_2)+(x_3,y_3)\right]=(x_1,y_1)+(x_2+x_3,y_2+y_3)=$$
$$=(x_1+(x_2+x_3),y_1+(y_2+y_3))=((x_1+x_2)+x_3,(y_1+y_2)+y_3)=$$
$$=\left[(x_1+x_2),(y_1+y_2)\right]+(x_3,y_3)=(z_1+z_2)+z_3,\ \forall z_1,z_2,z_3\in C$$

Propiedad conmutativa:

$$z_1+z_2=(x_1,y_1)+(x_2,y_2)=(x_1+x_2,y_1+y_2)=(x_2+x_1,y_2+y_1)=$$
$$=(x_2,y_2)+(x_1,y_1)=z_2+z_1,\ \forall z_1,z_2\in C$$

Propiedad de elemento neutro (elemento nulo):

$$\mathrm{O}=(0,0)\to\forall z\in C,\mathrm{O}+z=(0,0)+(x,y)=(0+x,0+y)=(x+0,y+0)=$$
$$=(x,y)=z,\text{ o sea: }\mathrm{O}+z=z+\mathrm{O}=z$$

Propiedad de elemento simétrico (elemento opuesto):

$$\forall(x,y)\in C,\exists(-x,-y)\in C/(x,y)+(-x,-y)=(x-x,y-y)=(0,0)$$

- Estructura de $C-\{(0,0)\}$ como grupo multiplicativo conmutativo $\left(C-\{(0,0)\},.\right)$:

Propiedad asociativa:

$$\forall z_1,z_2,z_3\in C-\{(0,0)\}$$
$$(z_1.z_2).z_3=\left[(x_1,y_1).(x_2,y_2)\right](x_3,y_3)=\left(x_1x_2-y_1y_2,x_1y_2+x_2y_1\right).(x_3,y_3)=$$
$$=\left((x_1x_2-y_1y_2)x_3-(x_1y_2+x_2y_1)y_3,(x_1x_2-y_1y_2)y_3+(x_1y_2+x_2y_1)x_3\right)=$$
$$=(x_1,y_1)\left(x_2x_3-y_2y_3,x_2y_3+x_3y_2\right)=(x_1,y_1)\left[(x_2,y_2).(x_3,y_3)\right]=z_1.(z_2.z_3)$$

Propiedad conmutativa:

$$\forall z_1,z_2\in C-\{(0,0)\}$$
$$z_1.z_2=(x_1,y_1).(x_2,y_2)=\left(x_1x_2-y_1y_2,x_1y_2+x_2y_1\right)=$$
$$\left(x_2x_1-y_2y_1,x_2y_1+x_1y_2\right)=(x_2,y_2).(x_1,y_1)=z_2.z_1$$

Propiedad de elemento neutro (elemento unidad):

$$u=(1,0)\to\forall z\in C-\{(0,0)\},u.z=(1,0).(x,y)=$$
$$=(1.x-0.y,1.y-0.x)=(x,y)=z,\text{ o sea: }u.z=zu=z$$

Propiedad de elemento simétrico (elemento inverso):

$$\forall(x,y)\in C-\{(0,0)\},\exists\left(\frac{x}{x^2+y^2},\frac{-y}{x^2+y^2}\right)\in C-\{(0,0)\}/(x,y).\left(\frac{x}{x^2+y^2},\frac{-y}{x^2+y^2}\right)=$$
$$=\left(\frac{x^2+y^2}{x^2+y^2},\frac{xy-yx}{x^2+y^2}\right)=(1,0)$$

- Distributividad del producto respecto a la suma:

$$\forall z_1, z_2, z_3 \in C,\ z_1.(z_2+z_3)=(x_1,y_1).(x_2+x_3,y_2+y_3)=$$
$$=(x_1(x_2+x_3)-y_1(y_2+y_3),x_1(y_2+y_3)+y_1(x_2+x_3))=$$
$$=((x_1x_2-y_1y_2)+(x_1x_3-y_1y_3),(x_1y_2+x_2y_1)+(x_1y_3+x_3y_1))=$$
$$=(x_1x_2-y_1y_2,x_1y_2+x_2y_1)+(x_1x_3-y_1y_3,x_1y_3+x_3y_1)=$$
$$=(x_1,y_1).(x_2,y_2)+(x_1,y_1).(x_3,y_3)=z_1.z_2+z_1.z_3$$

El conjunto C es, por tanto, un cuerpo conmutativo.

- C contiene una parte isomorfa a R:

Sea $C_R=\{(x,0)/x\in R\}$ y comprobemos que existe un isomorfismo $\psi: R\to C_R$ definido por la condición de que $\forall x\in R,\ \psi(x)=(x,0)\in C_R$.

a) Es aplicación:
$$\forall x\in R,\ \exists(x,0)\in C\to\forall x\in R,\ \exists(x,0)\in C_R/\ \psi(x)=(x,0)$$
b) Es inyectiva:
$$\psi(x)=\psi(y)\to(x,0)=(y,0)\to x=y$$
c) Es sobreyectiva:
$$\forall(x,0)\in C_R,\ \exists x\in R\to\forall(x,0)\in C_R,\ \exists x\in R/\ \psi(x)=(x,0)$$
d) Es homomorfismo:
$$\forall x,y\in R,\ \psi(x+y)=(x+y,0)=(x,0)+(y,0)=\psi(x)+\psi(y)$$
$$\forall x,y\in R,\ \psi(x.y)=(x.y,0)=(x,0).(y,0)=\psi(x).\psi(y)$$
$$\forall x\in R,\ \forall\alpha\in R,\ \psi(\alpha x)=(\alpha x,0)=\alpha(x,0)=\alpha\psi(x)\in C_R$$

Luego, tal aplicación es biyectiva y homomorfismo, es decir, es un isomorfismo de R en la parte C_R, llamada *complejos reales.*

- La unidad imaginaria:

Se denomina unidad imaginaria al número complejo $i=(0,1)$, el cual verifica que su cuadrado es el número real -1: $i^2=(0,1).(0,1)=(-1,0)\equiv -1$ (por isomorfismo). Esto permite resolver la ecuación $x^2+1=0\to x=\pm i$.

Todo número complejo puede expresarse en función de la unidad imaginaria:

$$\forall(x,y)\in C,\ (x,y)=(x,0)+(0,y)=x(1,0)+y(0,1)\equiv x.1+yi=x+iy$$

Construcción mediante extensiones algebraicas

Noción del concepto de ideal de un anillo:

De la teoría algebraica de anillos sabemos que para todo anillo *A*, un subgrupo *I* de *A* se dice ideal a la derecha (izquierda) si es multiplicativamente lícito a derecha (izquierda), o sea, si se verifica que

$$\forall x_1,x_2\in I,\ x_1-x_2\in I$$
$$\forall x\in I,\forall a\in A,\ xa\in I\ (derecha)$$
$$\forall x\in I,\forall a\in A,\ ax\in I\ (izquierda)$$

Si *I* es ideal a derecha y a izquierda simultáneamente diremos que se trata de un ideal bilátero, o simplemente, un ideal.

Un ejemplo de ideal bilátero del anillo de los números enteros es el conjunto de los múltiplos de 2: la diferencia de dos cualesquiera múltiplos de 2 es también múltiplo de 2, y el producto de un entero cualquiera por un múltiplo de 2 es también un múltiplo de 2.

Un ideal *I* es maximal del anillo A si cualquier ideal *I'* que le contenga es el mismo *I* o bien el anillo *A*:

$$I \text{ ideal maximal de A sii } I \subseteq I' \rightarrow I' = I \vee I' = A$$

Asimismo, para un anillo *A*, y para cualquier ideal bilátero de *A*, la relación *R* definida en *A* por la condición

$$aRb \leftrightarrow a - b \in I,\ a, b \in A$$

es una relación de equivalencia compatible con la estructura de anillo, y, por consiguiente, el conjunto cociente *A/R*, que acostumbra a designarse por *A/I*, es un anillo.

Un resultado clave del álgebra de anillos establece que si un anillo *A* tiene elemento unidad entonces la condición necesaria y suficiente para que el anillo cociente *A/I* sea un cuerpo es que *I* sea maximal.

El cuerpo $R[x]/(x^2+1)$:
Consideremos el anillo *R[x]* de los polinomios en una indeterminada con coeficientes en *R*. Y consideremos el polinomio irreducible $p(x) = x^2 + 1 \in R[x]$. Sea *(p)* el ideal constituido por los múltiplos de *p(x)*, el cual es, obviamente, ideal maximal del anillo $R[x]$.

Si definimos en $R[x]/(p)$ las operaciones suma y producto en la forma

$$\forall [p_1(x)+(p)], [p_2(x)+(p)] \in R[x]/(p):$$

$$[p_1(x)+(p)] + [p_2(x)+(p)] = [p_1(x)+p_2(x)] + (p)$$

$$[p_1(x)+(p)].[p_2(x)+(p)] = [p_1(x).p_2(x)] + (p)$$

es obvio que tiene estructura de cuerpo, pues siendo $p(x) = x^2 + 1$ irreducible, el ideal $(p(x)) \equiv (p)$ es maximal.

Dicho cuerpo, que llamaremos cuerpo de ruptura de $p(x) = x^2 + 1$, contiene una parte isomorfa al cuerpo *R* de los números reales como vemos en el siguiente teorema.

Sea $\varphi : R[x] \rightarrow R[x]/(p)$, definida por la condición

$$\forall \alpha(x) \in R[x], \varphi(\alpha(x)) = \alpha(x) + (p) \in R[x]/(p)$$

donde es
$(p) \equiv (x^2 + 1)$ ideal maximal del anillo $R[x]$ de polinomios en una indeterminada.

Si el polinomio es la indeterminada x, representaremos la imagen por ξ, es decir:
$\varphi(x) = x + (p) \equiv \xi$.

Si el polinomio es un nº real, $r \in R$, la imagen será $\varphi(r) = r + (p)$

Teorema:
La aplicación $\varphi : R[x] \to R[x]/(p)$ es homomorfismo.
Demostr.:

$$\forall \alpha(x), \beta(x) \in R[x],\ \varphi\big(\alpha(x)+\beta(x)\big) = \alpha(x)+\beta(x)+(p) =$$
$$= \big(\alpha(x)+(p)\big)+\big(\beta(x)+(p)\big) = \varphi(\alpha(x))+\varphi(\beta(x))$$
$$\forall \alpha(x), \beta(x) \in R[x],\ \varphi\big(\alpha(x).\beta(x)\big) = \alpha(x).\beta(x)+(p) =$$
$$= \big(\alpha(x)+(p)\big).\big(\beta(x)+(p)\big) = \varphi(\alpha(x)).\varphi(\beta(x))$$
$$\forall \alpha(x) \in R[x], \forall k \in R,\ \varphi\big(k.\alpha(x)\big) = k.\alpha(x)+(p) = k\big(\alpha(x)+(p)\big) = k.\varphi(\alpha(x))$$

La imagen de un polinomio de grado m es, por tanto:

$$\varphi\left(a_0 + a_1 x + \ldots + a_m x^m\right) = a_0 + a_1 x + \ldots + a_m x^m + (p)$$

o bien:

$$\varphi\left(a_0 + a_1 x + \ldots + a_m x^m\right) = a_0 + a_1\varphi(x) + \ldots + a_m\varphi(x)^m = a_0 + a_1\xi + \ldots + a_m\xi^m$$

Teorema:
Existe una parte R_φ del cuerpo $R[x]/(p)$ que es isomorfa a R.
Demostr.:
Si $r \in R, \varphi(r) = r + (p)$, por lo que si $r, s \in R / \varphi(r) = \varphi(s)$:

$$\left.\begin{array}{l} \varphi(r) = r + (p) \\ \varphi(s) = s + (p) \end{array}\right\} \to r + (p) = s + (p) \to r = s$$

Es decir, el homomorfismo φ es inyectivo en R, lo que indica que su imagen R_φ en $R[x]/(p)$ es isomorfa a R.
Tal imagen isomorfa R_φ está constituida por los elementos $\varphi(r) = r + (p)$, con *r* real.

Teorema:
La imagen en $R[x]/(p)$ del polinomio irreducible x^2+1 no es un polinomio irreducible.
Demostr.:
Se tiene que $\varphi(x^2+1) = (x^2+1)+(p)$, y siendo (p) el ideal de los múltiplos de x^2+1, será $\varphi(x^2+1) = (p) \equiv 0 + (p)$. En definitiva:

$$\left.\begin{array}{l} \varphi(x^2+1) = 0 + (p) \\ \varphi(x^2+1) = \xi^2 + 1 \end{array}\right\} \to \xi^2 + 1 = 0$$

Es decir, $\exists \xi \in R[x]/(p)$ tal que $\xi^2 + 1 = 0 \to \xi^2 = -1$

Teorema:
Los elementos del cuerpo $R[x]/(p)$ pueden representarse por pares de números reales. Tal representación es única.
Demostr.:
Sea un polinomio cualquiera $h(x)$ del anillo $R[x]$. Dividiendo por el polinomio irreducible x^2+1 se obtendrá un cociente $j(x)$ y un resto $r(x)$:

$$h(x)=(x^2+1).j(x)+r(x)$$

como el divisor es de grado 2, el resto será como máximo de grado 1: $r(x)=a+bx$.

Entonces:

$$\varphi(h(x))=\varphi\left((x^2+1).j(x)+r(x)\right)=\varphi\left((x^2+1).j(x)\right)+\varphi\left(r(x)\right)=$$

$$=\varphi(x^2+1).\varphi(j(x))+\varphi\left(r(x)\right)=0.\varphi(j(x))+\varphi\left(r(x)\right)=\varphi(r(x))=$$

$$=\varphi(a+bx)=\varphi(a)+b\varphi(x)=a+b\xi$$

Es decir:

$$\forall h(x)\in R[x],\ \exists(a,b)\in R^2 \text{ tal que } \varphi(h(x))=h(\xi)=a+b\xi$$

O dicho de otro modo:

$$\forall h(\xi)\in R[x]/(p),\ \exists(a,b)\in R^2 \text{tal que } h(\xi)=a+b\xi$$

Veamos que tal representación es única:

Si hubieran dos representaciones distintas del mismo elemento, $a+b\xi$ y $a'+b'\xi$, se tendría:

$$a+b\xi=a'+b'\xi\rightarrow(a-a')+(b-b')\xi=0\rightarrow\xi=-\frac{a-a'}{b-b'}=r\in R$$

y se cumpliría que $\xi^2=r^2>0$, lo cual es absurdo, pues sabemos que $\xi^2=-1$

En definitiva, el cuerpo de ruptura $R[x]/(p)$ resultar ser la extensión algebraica simple del cuerpo R de los números reales por la adjunción del elemento ξ:

$$\frac{R[x]}{(x^2+1)}=R(\xi)$$

Teorema:

Cualquiera que sea el polinomio $a_2x^2+a_1x+a_0\in R[x]$ irreducible, su cuerpo de ruptura es isomorfo al cuerpo de ruptura del polinomio $x^2+1\in R[x]$:

$$\frac{R[x]}{(a_2x^2+a_1x+a_0)}\approx\frac{R[x]}{(x^2+1)}$$

Demostr.:

- El cuerpo de ruptura de x^2+1 es la extensión algebraica simple $R(\xi)$, siendo ξ la raíz del polinomio en su cuerpo de ruptura.
- Análogamente, el cuerpo de ruptura del polinomio $a_2x^2+a_1x+a_0$ será la extensión algebraica simple $R(\eta)$, donde es η raíz de dicho polinomio en el cuerpo de ruptura.

Se tiene:

- Cualquiera que sea el signo del discriminante $a_1^2-4a_2a_0$ es

$$\eta=\frac{-a_1\pm\sqrt{a_1^2-4a_2a_0}}{2a_2}=A\pm B\xi\in R(\xi)\rightarrow\eta\in R(\xi)\rightarrow R(\eta)\subseteq R(\xi)$$

- Por otra parte

$$\eta=A+B\xi\rightarrow\xi=-\frac{A}{B}\pm\frac{1}{B}\eta\rightarrow\xi\in R(\eta)\rightarrow R(\xi)\subseteq R(\eta)$$

De ambas inclusiones, $R(\eta)=R(\xi)$y, por tanto:

$$\frac{R[x]}{(a_2x^2+a_1x+a_0)} \approx \frac{R[x]}{(x^2+1)}$$

Teorema:

El cuerpo de ruptura $\frac{R[x]}{(x^2+1)}$ es isomorfo al cuerpo de los números complejos.

Demostr.:

Puesto que cualquier elemento del cuerpo de ruptura se puede representar por un par ordenado de números reales, esto es $\forall h \in R(\xi),\ h = a + b\xi$, podemos definir la aplicación $\varphi : R(\xi) \to C$ por la condición $\forall h \in R(\xi),\ \varphi(h) = (a,b) \in C$.

Veamos que se trata de un isomorfismo de cuerpos:

a) Es aplicación:

$$\forall h \in R(\xi),\ h = a + b\xi \to \exists (a,b) \in R^2 \text{ único} / \varphi(h) = (a,b)$$

b) Es inyectiva:

$$\text{Si } \varphi(h) = (a,b) \wedge \varphi(l) = (c,d) / \varphi(h) = \varphi(l) \to (a,b) = (c,d) \to a = c,\ b = d \to h = l$$

c) Es sobreyectiva:

$$\forall (a,b) \in R^2, \exists h \in R(\xi) / h = a + b\xi \to \exists h \in R(\xi) / \varphi(h) = (a,b)$$

d) Es homomorfismo:

$$\forall h,l \in R(\xi), \varphi(h+l) = \left((a+b\xi)+(c+d\xi)\right) = \left((a+c)+(b+d)\xi\right) = \left(a+c,\ b+d\right) =$$
$$= (a,b)+(c+d) = \varphi(h)+\varphi(l)$$
$$\forall h,l \in R(\xi), \varphi(h.l) = \varphi\left((a+b\xi).(c+d\xi)\right) = \varphi\left((ac+(ad+bc)\xi+(bd)\xi^2\right) =$$
$$= \varphi(ac-bd+(ad+bc)\xi) = \left(ac-bd, ad+bc\right) = (a,b).(c,d) = \varphi(h)+\varphi(l)$$
$$\forall k \in R, \forall h \in R(\xi),\ \varphi(kh) = \varphi(k(a+b\xi)) = \varphi(ka+kb\xi) = (ka,kb) =$$
$$= k(a,b) = k\varphi(h)$$

Bibliografía

Apostol, Análisis Matemático, Reverté
Apostol, cálculus, Reverté
Queysanne, Algebra básica, Vicens Vives
Spivak, Calculus, Reverté
Birkhoff-McLane, Algebra moderna, Vicens Vives