Ayudantia 23

Profesor: Cristóbal Rivas
Ayudantes: Benjamin Martinez, Javier Pavez

Martes 22 de Noviembre 2022

0.1. Ejercicios para la ayudantía.

Ejercicio 23.1. Sean F_1 y F_2 subcuerpos de un cuerpo F. Definimos el composito de F_1 y F_2 al menor subcuerpo de F que contiene a F_1 y F_2, lo denotamos por F_1F_2. Demostrar que el composito de $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt[3]{2})$ es el cuerpo $\mathbb{Q}(\sqrt[6]{2})$. Recuerde que $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$.

Demostración. Para mostrar que $\mathbb{Q}(\sqrt[6]{2})$ es el composito, primero debemos mostrar que $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt[3]{2})$ están contenidos en $\mathbb{Q}(\sqrt[6]{2})$. Luego, debemos mostrar que si un subcuerpo de $\mathbb{R}$ contiene a $\mathbb{Q}(\sqrt{2})$ y $\mathbb{Q}(\sqrt[3]{2})$, entonces contiene a $\mathbb{Q}(\sqrt[6]{2})$.

1° Mostraremos que están contenidos en $\mathbb{Q}(\sqrt[6]{2})$ por definición de cuerpo generado. Dado que $\mathbb{Q}(\sqrt{2})$ (resp. $\mathbb{Q}(\sqrt[3]{2})$) es el menor cuerpo que contiene a los racionales y a $\sqrt{2}$ (resp. $\sqrt[3]{2}$), basta demostrar que $\sqrt{2}$ (resp. $\sqrt[3]{2}$) está en $\mathbb{Q}(\sqrt[6]{2})$.

Por definición $\sqrt[6]{2} \in \mathbb{Q}(\sqrt[6]{2})$. Como $\mathbb{Q}(\sqrt[6]{2})$ es un cuerpo, tendremos que $(\sqrt[6]{2})^3$, $(\sqrt[6]{2})^2 \in \mathbb{Q}(\sqrt[6]{2})$. O sea, $(\sqrt{2})$, $(\sqrt[3]{2}) \in \mathbb{Q}(\sqrt[6]{2})$. Por lo tanto, como ya tenemos por definición que $\mathbb{Q} \subset \mathbb{Q}(\sqrt[6]{2})$, concluimos que $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[6]{2})$ y $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[6]{2})$.

2° Denotamos por K a un cuerpo que contiene a $\mathbb{Q}(\sqrt{2})$ y a $\mathbb{Q}(\sqrt[3]{2})$. Mostraremos que $\mathbb{Q}(\sqrt[6]{2})$ está contenido en K.

Como $\mathbb{Q}(\sqrt{2}) \subset K$, inmediatamente tenemos que $\mathbb{Q} \subset K$. Por lo que solo nos falta probar que $\sqrt[6]{2} \in K$. Para eso, operaremos lo único que sabemos que está en K.

Por hipótesis $\sqrt{2}$, $\sqrt[3]{2} \in K$. Luego, $\sqrt{2} \cdot \sqrt[3]{2}$, $(\sqrt[3]{2})^2 \in K$. O sea, $\sqrt[6]{2^5}$, $\sqrt[6]{2^4} \in K$.
Antes de seguir recordemos que $\mathbb{Q}(\sqrt[3]{2})$ es un cuerpo contenido en los reales, como $2^{\frac{4}{6}} = 2^{\frac{2}{3}} = (2^{\frac{1}{3}})^2 = (\sqrt[3]{2})^2 \in \mathbb{Q}(\sqrt[3]{2})$. Tendremos necesariamente que el inverso multiplicativo, $2^{-\frac{4}{6}}$, está en $\mathbb{Q}(\sqrt[3]{2})$ y por lo tanto en K.
Así conseguimos decir que $\sqrt[6]{2} = 2^{\frac{1}{6}} = 2^{\frac{5}{6}} \cdot 2^{-\frac{4}{6}} = \sqrt[6]{2^5} \cdot 2^{-\frac{4}{6}} \in K$.

Finalmente deducimos que $\mathbb{Q}(\sqrt[6]{2})$ está contenido en K. Por lo tanto concluimos que $\mathbb{Q}(\sqrt[6]{2})$ es el menor subcuerpo de los reales que contiene a $\mathbb{Q}(\sqrt{2})$ y a $\mathbb{Q}(\sqrt[3]{2})$, es decir, su composito. □

Ejercicio 23.2. Demostrar que solo hay dos funciones que pueden ser ψ. Donde $\psi : \mathbb{C} \longrightarrow \mathbb{C}$ es un homomorfismo de anillos tal que $\psi \mid_{\mathbb{R}} = id$.

Demostración. Dado que todo complejo lo podemos escribir de la forma $a + bi$ con a, $b \in \mathbb{R}$, cuando escribamos con esa forma será un complejo cualquiera.

Tendremos que $\psi(a + bi) = \psi(a) + \psi(b)\psi(i) = a + b\psi(i)$, por lo que para saber cuantas funciones pueden ser ψ, nos preguntamos ¿a donde nuestro ψ puede mandar a i?

Para eso recordemos que el polinomio minimal de i en los reales es $p(x) = x^2 - 1$. Además notemos (1).

$$p(\psi(i)) = (\psi(i))^2 - 1 = \psi(i^2 - 1) = \psi(p(i)) = \psi(0) = 0 \tag{1}$$

Significa que $\psi(i)$ es una raiz de $p(x)$. Como las raíces de $p(x)$ son i y $-i$, tendremos que necesariamente $\psi(i) = i$ o $\psi(i) = -i$, ψ no puede mandar a i a ninguna otra parte.

Luego, tendremos que $\psi(a+bi) = a+bi$ o $\psi(a+bi) = a-bi$. Quien esté leyendo podrá corroborar que las dos reglas de asignaciones anteriores definen dos homomorfismos de anillos distintos entre si. Concluimos que solo dos funciones pueden ser ψ, las cuales son.

$$\begin{aligned} \psi_1 = id_{\mathbb{C}} : \mathbb{C} &\longrightarrow \mathbb{C}, \\ a+bi &\mapsto a+bi. \\ \psi_2 : \mathbb{C} &\longrightarrow \mathbb{C}, \\ a+bi &\mapsto a-bi. \end{aligned}$$

□

Lema 23.1. Sean A un cuerpo y B un anillo. Sea $\psi : A \longrightarrow B$ un homomorfismo de anillos. Demostrar que $\psi(A)$ es un cuerpo.

Demostración. Sabemos que $\psi(A)$ es un anillo. Mostraremos paso a paso lo que se necesita para llegar a cuerpo.

1° A conmutativo $\Rightarrow$ $\psi(A)$ conmutativo.

Como A es conmutativo, tendremos que $xy = yx$ para todo x, $y \in A$. Luego, $\psi(xy) = \psi(yx)$ para todo x, $y \in A$. Como ψ es un homomorfismo de anillos, $\psi(x)\psi(y) = \psi(y)\psi(x)$ para todo x, $y \in A$. Dado que $\psi(A) := \{\psi(x) \in B \mid x \in A\}$, de lo anterior concluimos que $zw = wz$ para todo z, $w \in \psi(A)$, es decir, $\psi(A)$ es conmutativo.

2° A es un anillo con unidad $\Rightarrow$ $\psi(A)$ es un anillo con unidad.

Como A es un anillo con unidad, existe $1 \in A$ tal que $1 \cdot x = x \cdot 1 = x$ para todo $x \in A$. Luego, $\psi(1 \cdot x) = \psi(x \cdot 1) = \psi(x)$ para todo $x \in A$. Dado que ψ es un homomorfismo de anillos, $\psi(1)\psi(x) = \psi(x)\psi(1) = \psi(x)$ para todo $x \in A$. Dado que $\psi(A) := \{\psi(x) \in B \mid x \in A\}$, de lo anterior concluimos que $\psi(1)z = z\psi(1) = z$ para todo $z \in \psi(A)$, es decir, $\psi(A)$ es un anillo con unidad.

Comentario: El que $\psi(1)$ sea el neutro multiplicativo de $\psi(A)$, no significa necesariamente que $\psi(1)$ sea el neutro multiplicativo de B. Como ejemplo basta considerar el siguiente homomorfismo de anillos.

$$\begin{aligned} \psi : \mathbb{Z} &\to M_{2\times 2}(\mathbb{Z}), \\ a &\mapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}. \end{aligned}$$

3° $u \in A$ es una unidad $\Rightarrow$ $\psi(u) \in \psi(A)$ es una unidad.

Denotemos por 1 al neutro multiplicativo de A. De 2° sabemos que $\psi(1)$ es el neutro multiplicativo de $\psi(A)$. Como $u \in A$ es una unidad, entonces existe $u^{-1} \in A$ tal que $u \cdot u^{-1} = u^{-1} \cdot u = 1$. Luego, $\psi(u \cdot u^{-1}) = \psi(u^{-1} \cdot u) = \psi(1)$. Como ψ es un homomorfismo de anillos, tendremos que $\psi(u)\psi(u^{-1}) = \psi(u^{-1})\psi(u) = \psi(1)$. Deducimos que $\psi(u^{-1})$ es el inverso multiplicativo de $\psi(u)$. Concluimos que $\psi(u)$ es una unidad.

4° Conclusiones.

Si A es un cuerpo, es un anillo conmutativo con unidad y todos sus elementos menos el 0 son unidades. Luego, por 1° y 2° tenemos que $\psi(A)$ es un anillo conmutativo y con unidad. Dado que $\psi(A) = \{\psi(x) \in B \mid x \in A\}$ y por 3°, tendremos que todo elemento menos $\psi(0)$ es una unidad.

Concluimos que $\psi(A)$ es un cuerpo. □

Ejercicio 23.3. Sea A un subanillo con unidad de un cuerpo k. Muestre que $A(S)$ es isomorfo a $Frac(A[S])$.

Demostración. Como $A(S)$ es por definición un anillo que contiene a A y a S, tendremos que $A[S]$ está contenido en $A(S)$, así quien esté leyendo puede corroborar que $\iota : A[S] \to A(S)$, $c \mapsto c$ es un homomorfismo de anillos inyectivo. Luego, por la Proposición 2.47. de los apuntes del curso tenemos que $\varphi : Frac(A[S]) \to A(S)$, $[a, b] \mapsto a \cdot b^{-1}$, es un homomorfismo de anillos inyectivo. Así solo nos falta mostrar que φ es sobreyectiva.

Para eso consideramos $B = \varphi(Frac(A[S]))$. Sabemos que φ es sobreyectiva si y solo si $B = A(S)$, por lo que a eso queremos llegar. Para esto usaremos lo único que sabemos de $A(S)$, es el menor cuerpo que contiene a A y a S. Basta entonces mostrar que B es un cuerpo que contiene a A y a S, y como $B \subset A(S)$ tendremos necesariamente que $B = A(S)$.

Notemos que $\varphi([a, 1]) \in B$ para todo $a \in A[S]$. Luego, $a \in B$ para todo $a \in A[S]$. Deducimos que $A[S] \subset B$ y en particular A, $S \subset B$. Además, como $Frac(A[S])$ es un cuerpo, tendremos por el Lema 23.1. que B es un cuerpo. O sea, conseguimos mostrar que B es un cuerpo que contiene a A y a S.
Finalmente, dado que por definición $B \subset A(S)$, pero $A(S)$ es la intersección de todos los cuerpo que contienen a A y a S, tendremos necesariamente que $B = A(S)$. Deduciendo que φ es sobreyectivo, y por lo tanto concluimos que $Frac(A[S]) \cong A(S)$.

□

0.2. Ejercicios para la casita.

Ejercicio 23.4. Sea K una extensión de un cuerpo F, $\alpha \in K$ y $b \in F$.

a) Demostrar que $F(b + \alpha) = F(\alpha)$

b) Si b es no nulo, entonces $F(ba) = F(a)$.

Ejercicio 23.5. Suponga que R y S son anillos isomorfos. Demuestre que $R[x] \cong S[x]$.

Ejercicio 23.6. Demuestre o refute: $x^p + a$ es irreducible para cualquier $a \in \mathbb{Z}/p\mathbb{Z}$, donde p es primo.

Ejercicio 23.6. ¿Cual de los siguientes polinomios son irreducibles sobre $\mathbb{Q}[x]$?

a) $x^4 - 2x^3 + 2x^2 + x + 4$.

b) $x^4 - 5x^3 + 3x - 2$.

c) $3x^5 - 4x^3 - 6x^2 + 6$.

d) $5x^5 - 6x^4 - 3x^2 + 9x - 15$.

e) $x^n - p$, con n, $p \in \mathbb{Z}$ y p número primo.