Universidad de Valladolid
Facultad de Ciencias

TRABAJO FIN DE GRADO

Grado en Matemáticas

Un Curioso Ejemplo: Anillos no Isomorfos con Anillos de Polinomios Isomorfos

Autor: Laura Esteban Sanz

Tutor: Manuel Carnicer Arribas

Índice general

Introducción

En 1972, la Sociedad Americana de Matemáticas (AMS) publica el artículo "*NONUNIQUENESS OF COEFFICIENT RINGS IN A POLYNOMIAL RING*", del matemático neoyorkino Melvin Hochster. En esta publicación se presenta un curioso ejemplo de dos anillos conmutativos y unitarios $\mathcal{B}$ y $\mathcal{C}$ tales que, siendo $\mathcal{B}$ y $\mathcal{C}$ no isomorfos, al considerar una indeterminada t, resulta que $\mathcal{B}[t] \cong \mathcal{C}[t]$.

El objetivo de este Trabajo de Fin de Grado es desarrollar la teoría que servirá de base para el resultado citado en el artículo. Por un lado, al probar un isomorfismo entre dos anillos de polinomios sobre distintos anillos de coeficientes, se realiza un estudio de algunas construcciones sobre módulos, habituales del álgebra conmutativa: Producto Tensorial, Álgebra Tensorial, Álgebra Simétrica, y sucesiones exactas escindidas. De la misma forma, para probar que los anillos de coeficientes de partida no son isomorfos debemos introducir nuevos conceptos matemáticos: automorfismos del cuerpo de los números reales, construcciones de pre-órdenes, e incluso se introduce un teorema geométrico conocido como Teorema de Poincaré.

El trabajo está estructurado en cuatro capítulos. En el primer capítulo, debemos empezar por unas nociones básicas de álgebra. Se darán por conocidos los conceptos y resultados sobre Anillos y Módulos conmutativos del primer capítulo y las cuatro primeras secciones del segundo capítulo del libro [1]. Como podemos observar, este libro se centra en el álgebra Conmutativa. Sin embargo, habrá ocasiones en las que no consideremos necesariamente un anillo conmutativo. El primer paso será, por tanto, construir la teoría sobre anillos no conmutativos y sus respectivos ideales bilaterales. Continuaremos con la definición y resultados sobre anillos graduados y módulos graduados. Después, la definición del Producto Tensorial de módulos y de álgebras.

En el segundo se quiere llegar a la construcción del Álgebra Simétrica. Con los resultados del primer capítulo, podemos así construir el Álgebra Tensorial. Después, definiremos el Álgebra Simétrica y veremos sus propiedades de funtorialidad, que nos serán de utilidad en el capítulo 4. Además, como nuestro objetivo es el ejemplo que aparece en el artículo, se prestará especial atención al Álgebra Simétrica de una suma directa de módulos.

El tercer capítulo está destinado a la presentación del teorema geométrico conocido como Teorema de Poincaré. Continuando con la asginatura de "Geometría de Curvas y Superficies" se enuncia el Teorema de Gauss-Bonnet, primero en su versión local y depués en su versión más general para regiones regulares. Como una aplicación de este último a los campos de vectores sobre superficies obtenemos el Teorema de Poincaré que enuncia que: Todos los campos de vectores con singularidades aisladas de una superficie homeomorfa a la esfera $\mathbb{S}^2$ deben cumplir que la suma de sus índices sea igual a la característica de Euler de la esfera. Para este capítulo seguiremos la notación y terminología del libro [5].

Finalmente, en el Capítulo 4 desarrollaremos el ejemplo del artículo basándonos en los resultados previamente estudiados. Los resultados sobre Álgebra Simétrica vistos en el capítulo 2 nos permitirán establecer el isomorfismo entre los $\mathcal{A}$-módulos $\mathcal{B}[t] = \mathcal{A}[P, Q, t]$ y $\mathcal{C}[t] = S(\mathbb{E})[t]$, donde $\mathcal{A}$ será el anillo $\mathcal{A} = \mathbb{R}[X, Y, Z]/(X^2 + Y^2 + Z^2 - 1)$, y $\mathbb{E}$ es el núcleo del homomorfismo $\Phi : \mathcal{A}^3 \to \mathcal{A}$ definido por $\Phi(a, b, c) = ax + by + zc$ para $(a, b, c) \in \mathcal{A}^3$. El Teorema de Poincaré nos permitirá demostrar que $\mathbb{E}$ debe tener, al menos, 3 generadores. Este resultado nos llevará a una contradicción por la que finalmente concluiremos que $\mathcal{B}$ y $\mathcal{C}$ no son isomorfos. En el camino para obtener esta contradicción necesitaremos trabajar con sucesiones escindidas, así como con los automorfismos de $\mathbb{R}$ y la construcción de pre-órdenes.

Capítulo 1

Primeras nociones

En este capítulo se darán por conocidos los conceptos y resultados sobre Anillos y Módulos conmutativos del primer capítulo y las cuatro primeras secciones del segundo capítulo del libro [1].

1.1. Anillos no conmutativos

Definición 1.1.1. Un anillo $(A, +, \cdot)$ es un conjunto A dotado de dos operaciones internas, suma $(x, y) \mapsto x + y$, y multiplicación $(x, y) \mapsto x \cdot y$, que cumplen las siguientes propiedades:

1. Para la suma, A es un grupo conmutativo.
2. La multiplicación cumple la propiedad de asociatividad.
3. La multiplicación es distributiva con respecto de la suma.
4. Si la multiplicación tiene la propiedad conmutativa, el anillo A es un *anillo conmutativo.*
5. Si la multiplicación posée elemento neutro, es decir, existe un único elemento $1 \in A$ tal que $x1 = 1x = x$ para todo $x \in A$, el anillo A es un *anillo unitario.* Denotaremos el elemento neutro como 1_A o 1 si no hay lugar a confusión.

Nota

De aquí en adelante consideraremos todos los anillos unitarios. Recordemos también que el elemento neutro es único.

Definición 1.1.2. El conjunto A dotado solamente de la adición es un grupo conmutativo que se denomina grupo aditivo de A.

Definición 1.1.3. Sea A un anillo unitario. Llamaremos elemento unidad de A a un $a \in A$ tal que $ay = ya = 1$ para algún $y \in A$. A este elemento y le llamaremos inverso de a y lo denotaremos por a^{-1}.

Proposición 1.1.1. *Dado un anillo A y un elemento unidad $a \in A$. El inverso de a es único.*

Demostración. Supongamos $b \in A$ otro inverso de A. Entonces,

$$b = b1 = b(aa^{-1}) = (ba)a^{-1} = 1a^{-1} = a^{-1}$$

□

Definición 1.1.4. Dados dos anillos A y B, se define un homomorfismo de anillos f como una aplicación $f : A \to B$ tal que

I. $f(x + y) = f(x) + f(y)$ para $x, y \in A$.

II. $f(xy) = f(x)f(y)$ para $x, y \in A$.

III. $f(1_A) = 1_B$.

Definición 1.1.5. Sea A un anillo. Se define un ideal por la izquierda (resp. por la derecha) como un subgrupo del grupo aditivo de A tal que si $a \in A$ y $x \in I$ se tiene que $ax \in I$ (resp. $xa \in I$). Si un ideal es a la vez un ideal por la derecha y por la izquierda de A, se denominará ideal biláteró o bilateral de A.

Aunque tenemos una nueva definicón de ideal bilateral para el caso de anillos no conmutativos, las propiedades de ideales se conservan:

Proposición 1.1.2. *Sea A un anillo. La intersección de ideales biláteros de A es un ideal bilateral de A*

Demostración. Sea (I_j) una colección de ideales biláteros de A. Es claro que la interseción es un subgrupo aditivo. Por otro lado, si $x \in A$ y $a \in \cap I_j$ se tiene que $xa \in I_j$ y $ax \in I_j$ para cada j por ser ideales biláteros. Y por tanto, $xa \in \cap I_j$ y $ax \in \cap I_j$. Entonces, la intersección es un ideal bilateral.

□

Definición 1.1.6. Dado un anillo A y un subconjunto $S \subset A$. Se define el ideal bilateral generado por el conjunto S como la intersección de todos los ideales bilaterales de A que contienen a S.

Proposición 1.1.3. *Dado un anillo A y un subconjunto $S \subset A$. El conjunto de todas las combinaciones lineales de elementos de S con coeficientes en A, este es $\langle S \rangle = \{\sum_{j=1}^{n} a_j x_j b_j | a_j, b_j \in A, x_j \in S\}$, es el ideal biláteró generado por S.*

Demostración. Sea $\langle S \rangle = \{\sum_{j=1}^{n} a_j x_j b_j | a_j, b_j \in A, x_j \in S\}$.
Veamos, en primer lugar, que $\langle S \rangle$ es un ideal bilateral. Tenemos $0 = 0x0$ para cualquier $x \in S$, luego $0 \in \langle S \rangle$. Tomando dos elementos $s_1 = \sum a_j x_j b_j$ y $s_2 = \sum a'_i x'_i b'_i \in \langle S \rangle$, veamos que su resta está en $\langle S \rangle$.

$$s_1 - s_2 = \sum a_i x_i b_i - \sum a_j x_j b_j = \sum a_i x_i b_i + \sum (-a_j) x_j b_j$$

que es una suma finita de las que pertenecen a $\langle S\rangle$, luego es un subgrupo aditivo de A. Además, si multiplicamos por un elemento calquiera $a \in A$ un elemento $s = \sum a_j x_j b_j$ de $\langle S\rangle$ se tiene $as = a(\sum a_j x_j b_j) = \sum (aa_j)x_j b_j$ que está en $\langle S\rangle$ porque el elemento aa_j está en A. Y si tomamos un elemento $s = \sum a_j x_j b_j$ de $\langle S\rangle$ multiplicado por un elemento cualquiera $a \in A$ entonces se tiene $(\sum a_j x_j b_j)a = \sum a_j x_j (b_j a)$ que está en $\langle S\rangle$ por ser A un anillo. Por tanto, $\langle S\rangle$ es un ideal.
Además, todo ideal bilatero que contenga a S debe contener a las combinaciones lineales de elementos de S. Veamos que $\langle S\rangle$ es el menor de todos los ideales de A que contienen a S. Todo elemento $x \in S$ es de la forma $x = 1x1$ con $1 \in A$, luego $S \subset \langle S\rangle$. Sea ahora I un ideal bilátero de A tal que $S \subset I$, $a_1, \dots, a_n, b_1, \dots, b_n \in A$ y $x_1, \dots, x_n \in S$. Por ser I un ideal, $a_j x_j b_j$ está en I, luego $\sum a_j x_j b_j$ está en I y se tiene $\langle S\rangle \subset I$.

□

Definición 1.1.7. Sea A un anillo. Si I es un ideal bilateral de A, se dice que dos elementos x e y de A son congruentes módulo I y se denota $x \equiv y \pmod I$, si $x - y \in I$.

Proposición 1.1.4. *Sea A un anillo e I un ideal bilátero de este, con la congruencia módulo I definida anteriormente se obtiene una relación de equivalencia en A.*

Demostración. Veamos que se cumplen las tres propiedades de una relación de equivalencia:

- Reflexiva. $\forall\, x \in A$, $x - x = 0 \in I$ por ser I ideal bilateral, luego $x \equiv x \pmod I$.
- Simétrica. $\forall\, x, y \in A$ tal que $x \equiv y \pmod I$, $x - y \in I$ y $-(x-y) = y - x \in I$ por ser I ideal bilateral. Luego $y \equiv x \pmod I$.
- Transitiva. $\forall\, x, y, z \in A$ tal que $x \equiv y \pmod I$ e $y \equiv z \pmod I$ entonces $x - y \in I$ y $y - z \in I$. Por ser I ideal bilateral $(x-y)+(y-z) = x - z \in I$. Luego $x \equiv z \pmod I$.

□

Proposición 1.1.5. *Sea A un anillo e I un ideal bilateral de A, el conjunto cociente de A por la relación de equivalencia $x \equiv y \pmod I$ dotado de la suma y de la multiplicación, denotado por A/I, es un anillo.*

Demostración. Denotamos por $(x + I)$ la clase de equivalencia del elemento $x \in A$ en A/I.
Para la suma, definida por

$$(x + I) + (x' + I) = (x + x') + I$$

A/I es el grupo conmutativo cociente del grupo aditivo de A sobre el subgrupo I. Es una operación que no depende de los representantes ya que de las relaciones $x \equiv y \pmod I$ y $x' \equiv y' \pmod I$ se tiene que

$$x - y \in I, x' - y' \in I \Rightarrow (x - y) + (x' - y') = (x + x') - (y + y') \in I$$

y se deduce que $x + x' \equiv y + y' \pmod I$.
En A/I la multiplicación definida por

$$(x + I)(x' + I) = (xx') + I$$

es una operación binaria interna que no depende de los representantes. Se tiene $x \equiv y \pmod I$ y $x' \equiv y' \pmod I$ luego $x - y \in I \Rightarrow x = y + b, b \in I$ y $x' - y' \in I \Rightarrow x' = y' + c, c \in I$. De esto se deduce que $xx' \equiv xy' (\mathrm{mod}\ I)$ dado que I es un ideal por la izquierda, y $xy' \equiv yy' \pmod I$ dado que I es también ideal por la derecha. Luego,

$$xx' = (y + b)(y' + c) = yy' + yc + by + bc$$

y como $yc \in I$, $by \in I$ y $bc \in I$ se deduce que $xx' = yy' \pmod I$. Esta multiplicación cumple la propiedad asociativa y tiene elemento neutro $(1 + I)$ donde 1 es el elemento neutro del anillo A.

$$(x+I)((y+I)(z+I)) = (x+I)(yz+I) = (x(yz)+I) = ((xyz)+I) = (xy+I)+(z+I) =$$
$$= ((x + I)(y + I))(z + I)$$

De igual forma, se cumple la propiedad distributiva de la multiplicación con respecto de la suma.

$$(x+I)((y+I)+(z+I)) = (x+I)((y+z)+I) = (x(y+z)+I) = ((xy+xz)+I) =$$
$$= (xy + I) + (xz + I) = (x + I)(y + I) + (x + I)(z + I)$$

$\square$

Definición 1.1.8. Sea A un anillo e I un ideal bilateral de A. Llamaremos anillo cociente de A por I y lo denotamos por A/I al conjunto cociente de A por la relación de equivalencia $x \equiv y \pmod I$ dotado de la suma y de la multiplicación cociente de aquellas en A.

Nota
Como se ha visto en la demostración anterior, si el anillo A es un anillo unitario, también lo será el anillo cociente A/I.

1.2. Anillos graduados y módulos graduados.

Definición 1.2.1. Sea A un anillo. Llamaremos graduación en A a una descomposición del grupo aditivo de la forma $A = \bigoplus_{n \geq 0} A_n$ como suma directa de subgrupos de A tales que $A_m A_n \subseteq A_{m+n}$ para todo $m, n \geq 0$.
Llamaremos anillo graduado a un anillo A con una graduación.

Ejemplos

1. El caso en el que $A_0 = A$ y $A_n = 0$ para $n > 0$, se llama graduación trivial de A.

2. El anillo de polinomios $A = k[X_1, \ldots, X_r]$ sobre un anillo k es graduado si consideramos A_n como el k-submódulo de los polinomios homogéneos de grado n. En particular, $A_0 = k$. A esta graduación la llamaremos graduación usual en A.

3. También se puede considerar una graduación ponderada en el anillo de polinomios A atribuyendo los grados $\omega_1, \ldots, \omega_r \in N$ a las variables. En este caso, A_n es el k-submódulo generado por los monomios de grado n, es decir, $X_1^{\alpha_1} \cdot \cdots \cdot X_r^{\alpha_r}$ tales que $\alpha_1\omega_1 + \cdots + \alpha_r\omega_r = n$. La graduación usual es un caso particular de la graduación ponderada tomando los grados $1, \ldots, 1$.

Definición 1.2.2. Sea $A = \bigoplus_{n\geq 0} A_n$ un anillo graduado. El grupo A_n se llamará componente homogénea de grado n de A y los elementos de A_n son los elementos homogéneos de grado n.

Nota.
Sea $A = \bigoplus_{n\geq 0} A_n$ un anillo graduado. El elemento 0 es un elemento homogéneo de cualquier grado. Es trivial dado que los A_n son subgrupos.

Definición 1.2.3. Sea $A = \bigoplus_{n\geq 0} A_n$ un anillo graduado. Para cada $a \in A$ llamaremos descomposición homogénea de a a la expresión $a = \sum_{n\geq 0} a_n$ donde $a_n \in A_n$ para cada n y $a_n = 0$ para casi todas las n salvo un número finito. El elemento a_n es la componente homogénea de grado n de a.

Lema 1.2.1. *Sea $A = \bigoplus_{n\geq 0} A_n$ un anillo graduado. Para cada $a \in A$, la descomposición homogénea $a = \sum_{n\geq 0} a_n$ es única.*

Demostración. Supongamos $a = \sum_{n\geq 0} b_n$ otra descomposición homogénea de a con $b_n \in A_n$. Entonces,

$$a = \sum_{n\geq 0} a_n = \sum_{n\geq 0} b_n$$

Restando las componentes de grado j,

$$b_j - a_j = \sum_{n\neq j} (b_n - a_n)$$

Como la resta de dos componenetes de grado j está en la componente A_j, la suma $\sum_{n\neq j} (b_n - a_n)$ también debería estar en la componente A_j. Pero esto no se puede dar salvo que $b_j - a_j = 0$. Luego $b_j = a_j$ para todo $j = 1, \cdots, n$.

□

Proposición 1.2.1. *Sea* $A = \bigoplus_{n\geq 0} A_n$ *un anillo graduado. La componente* A_0 *es un subanillo de* A*, y cada* A_n *es un* A_0*-submódulo de* A*.*

Demostración. Para probar que A_0 es subanillo de A tenemos que ver que es cerrado para la suma y la multiplicación y que contiene el elemento neutro $1 \in A$. La componente homogénea A_0 es cerrada para la multiplicación ya que se tiene $A_0A_0 \subset A_0$. Escribiendo $1 = \sum_{n\geq 0} a_n$ con $a_n \in A_n$ se tiene entonces que $a_i = 1a_i = \sum_{n\geq 0} a_n a_i$. Comparando las componentes homogéneas de grado i se tiene $a_i = a_0 a_i$ y $a_0 = a_0 1 = \sum_{i\geq 0} a_0 a_i = \sum_{i\geq 0} a_i = 1$, probando que $1 \in A_0$ y por tanto A_0 es subanillo de A. El hecho de que A_n sea un A_0-submódulo de A se deduce de que $A_0 A_n \subseteq A_n$.

□

Definición 1.2.4. Sean A y B dos anillos graduados, diremos que un homomorfismo de anillos $f : A \to B$ es graduado si $f(A_n) \subseteq B_n$ para cada $n \geq 0$.

Lema 1.2.2. *Sea* $A = \bigoplus_{n\geq 0} A_n$ *un anillo graduado e* I *un ideal bilatero de* A*. Las condiciones siguientes son equivalentes:*

1. *Para cada* $a \in I$ *todas las componentes homogéneas de* a *están en* I*.*
2. $I = \bigoplus_{n\geq 0} (I \cap A_n)$*.*
3. *El ideal* I *está generado por elementos homogéneos.*

Demostración.

- $1 \Rightarrow 2$.
  La descomposición homogénea del elemento a se escribe como $a = \sum_{n\geq 0} a_n$ y por 1. se tiene que $a_n \in I \cap A_n$ para todo n y esta descomposición es única. Por ello se tiene $I \subseteq \sum_{n\geq 0} (I \cap A_n)$ y como $(I \cap A_n) \cap (\sum_{i\neq n} (I \cap A_i)) = 0$ entonces $I = \bigoplus_{n\geq 0} (I \cap A_n)$.

- $2 \Rightarrow 3$.
  Por la expresión en 2. I está generado por $\bigcup_{n\geq 0} (I \cap A_n)$ que es un conjunto de elementos homogéneos.

- $3 \Rightarrow 1$.
  Supongamos que I está generado por un conjunto S de elementos homogéneos. Sea $a \in I$, para $n \geq 0$ se considera la componente homogénea de a de grado n y queremos ver que $a_n \in I$. Se tiene

  $$a = b_1 s_1 t_1 + \cdots + b_r s_r t_r$$

  para $s_1, \ldots, s_r \in S$ y $b_1, \ldots, b_r, t_1, \ldots, t_r \in A$. Si $b_i = \sum_j b_{ij}$ y $t_k = \sum_l t_{kl}$ son las respectivas descomposiciones homogeneas de b_i y de t_k donde los

$b_{ij} \in A_j$ (A_j la componente homogénea de A de grado j), $t_{kl} \in A_l$. Entonces, teniendo en cuenta las componentes homogéneas de grado n, si suponemos $b_{ij} = 0$ cuando $j < 0$ y análogamente lo suponemos para t_{kl} y si llamamos d_i al grado de s_i, se tiene que

$$a_n = \sum_i \sum_{j+l+d_i=n} b_{ij} s_i t_{il} \in I$$

$\square$

Definición 1.2.5. Entenderemos por ideal homogéneo de un anillo graduado A a un ideal de A que satisface una de las condiciones equivalentes del lema anterior.

Nota

Si $A = \bigoplus_{n \geq 0} A_n$ es un anillo graduado e I es un ideal homogéneo de A denotamos $I_n = I \cap A_n$. Entonces, el anillo cociente A/I hereda la graduación cociente dada por $(A/I)_n = A_n/I_n$. Es decir $A/I = \bigoplus_{n \geq 0} A_n/I_n$. Con esta graduación, el homomorfismo de anillos $f : A \to A/I$ es un homomorfismo de anillos graduado.

Definición 1.2.6. De forma análoga, si A es un anillo graduado, llamaremos A-módulo graduado a un A-módulo M con la descomposión como grupo conmutativo $M = \bigoplus_{n \geq 0} M_n$ de subgrupos de M tales que $A_m M_n \subseteq M_{m+n}$ para todo $m, n \geq 0$.

Definición 1.2.7. Llamaremos componente homogénea de grado n de M al subgrupo M_n para algún $n \geq 0$ y entonces, cada elemento de M_n es un elemento homogéneo de grado n de M. Cada $x \in M$ puede escribirse de forma única como suma $\sum_{n \geq 0} x_n$ donde $x_n \in M_n$ y todas las x_n salvo un número finito de ellas son 0. Esta expresión es la descomposición homogénea de x y las x_n se llamarán componenetes homogéneas de grado n de x.

Definición 1.2.8. Sean M y N dos A-módulos graduados, y sea d un número entero. Diremos que un homomorfismo de A-modulos $f : M \to N$ es graduado de grado d si $f(M_n) \subseteq N_{n+d}$ para todo $n \geq 0$.

Lema 1.2.3. *Sea $M = \bigoplus_{n \geq 0} M_n$ un módulo graduado y N un submódulo de M. Las condiciones siguientes son equivalentes:*

1. *Para cada $x \in N$ todas las componentes homogéneas de x están en N.*
2. *$N = \bigoplus_{n \geq 0} (N \cap M_n)$.*
3. *El A-módulo N está generado por elementos homogéneos.*

Demostración. La demostración es análoga a la del Lema 1.2.2 pero para el caso de A-módulos.

$\square$

Definición 1.2.9. Llamaremos submódulo graduado de un A-módulo graduado M a un submódulo N que cumpla una de las condiciones equivalentes del lema anterior.

Nota
Si $M = \bigoplus_{n \geq 0} M_n$ es un módulo graduado y N es un submódulo graduado de M, el módulo cociente M/N hereda la graduación cociente dada por

$$(M/N)_n = M_n/N_n$$

donde $N_n = N \cap M_n$. Con esta graduación, el homomorfismo $f : M \to M/N$ es un homomorfismo graduado de grado cero.

1.3. Álgebras.

Definición 1.3.1. Sea B un anillo. Denominaremos centro de B al subanillo

$$centroB = \{b \in B | bx = xb \quad \forall x \in B\}$$

Definición 1.3.2. Sea A un anillo conmutativo. Definiremos una A-álgebra B como un anillo B junto con un homomorfismo de anillos $f : A \to B$ tal que $f(A) \subseteq centroB$. Diremos que el álgebra es conmutativa si el anillo B es conmutativo.

Definición 1.3.3. El homomorfismo f se denomina homomorfismo estructural del A-álgebra B. Por ello, también diremos que el par (B, f) con $f : A \to B$ es una A-álgebra.

Ejemplos.

1. Todo anillo conmutativo A es una $\mathbb{Z}$-álgebra de forma única ya que existe un único homomorfismo de anillos $\mathbb{Z} \to A$ determinado por $1 \mapsto 1_A$.

2. Si A es un subanillo de un anillo conmutativo B, entonces B es una A-álgebra con la inclusión $A \hookrightarrow B$.

3. Si A es un anillo conmutativo y J es un ideal del anillo de polinomios en n variables $A[X_1, \ldots X_n]$, entonces $A[X_1, \ldots X_n]/J$ es una A-álgebra cuyo homomorfismo estructural es la composición de la inclusión

$$A \hookrightarrow A[X_1, \ldots X_n]$$

y la aplicación de paso al cociente

$$A[X_1, \ldots X_n] \to A[X_1, \ldots X_n]/J$$

Proposición 1.3.1. *Dada una A-álgebra B con su homomorfismo de anillos correspondiente $f : A \to B$. Entonces, f convierte al anillo B en un A-módulo.*

Demostración. Sea $f : A \to B$ el homomorfismo de anillos. Si $a \in A$ y $b \in B$, se define un producto externo

$$ab = f(a)b$$

Entonces, si $a, a_1, a_2 \in A$ y $b, b_1, b_2 \in B$ se cumple las propiedades de módulo:

$$a(b_1 + b_2) = f(a)(b_1 + b_2) = f(a)b_1 + f(a)b_2 = ab_1 + ab_2$$

$$(a_1 + a_2)b = f(a_1 + a_2)b = f(a_1)b + f(a_2)b = a_1b + a_2b$$

$$(a_1a_2)b = f(a_1a_2)b = f(a_1)f(a_2)b = f(a_1)(a_2b) = a_1(a_2b)$$

$$1_Ab = f(1_A)b = 1_Bb = b$$

□

Nota.
Además, se tiene $f(a) = f(a1_A) = f(a)f(1_A) = f(a)1_B = a1_B$, y este módulo cumple que, como $f(A) \subseteq centroB$, entonces para todo $a_1, a_2 \in A$ y $b_1, b_2 \in B$,

$$f(a_1a_2)b_1b_2 = f(a_1)f(a_2)b_1b_2 = f(a_1)b_1f(a_2)b_2$$

de donde se obtiene

$$(a_1a_2)(b_1b_2) = (a_1b_1)(a_2b_2)$$

Análogamente, si suponemos que un anillo B es un A-módulo con una multiplicación escalar satisfaciendo que para todo $a_1, a_2 \in A$ y $b_1, b_2 \in B$ entonces

$$(a_1a_2)(b_1b_2) = (a_1b_1)(a_2b_2)$$

se define $f : A \to B$ como $f(a) = a1_B$ para $a \in A$. De esta forma, f es un homomorfismo de anillos y $f(A) \subseteq centroB$:

$$xf(a) = 1_Bxf(a) = f(1_A)xf(a) = 1_A1_Bxa1_B = (1_Ax)(a1_B) = (1_Aa)(x1_B) =$$

$$= ax = a1_Bx = f(a)x$$

Así, dotamos a B con la estructura de A-álgebra cuyo homomorfismo estructural es f.

Definición 1.3.4. Sea A un anillo conmutativo y sean B y B' dos A-álgebras. Un homomorfismo de álgebras $h : B \to B'$ se define como un homomorfismo de anillos que también es homomorfismo de A-módulos.

Definición 1.3.5. Sea A un anillo graduado. Una A-álgebra B es una álgebra graduada si se tiene una descomposición como grupo conmutativo en suma directa de A-módulos de la forma $B = \bigoplus_{n \geq 0} B_n$ ($AB_n \subseteq B_n$) tales que cumplen $B_nB_m \subseteq B_{n+m}$. Los elementos de B_n se llaman elementos homogéneos de grado n.

1.4. Sucesiones exactas y Lema de escisión.

Definición 1.4.1. *Dada una sucesión finita o infinita de A-homomorfismos.*

$$\cdots \longrightarrow M_{i+1} \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} M_{i-1} \longrightarrow \ldots$$

Diremos que la sucesión es exacta en M_i si $Im(f_{i+1}) = Ker(f_i)$. Se denominará sucesión exacta si la sucesión es exacta en cada M_i.

Lema 1.4.1. *Una sucesión $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ es exacta si y sólo si f es inyectiva, g es sobreyectiva e $Im(f) = Ker(g)$. Además, en este caso, f induce un isomorfismo $M' \cong f(M')$, y g induce otro isomorfismo $M'' \cong M/f(M')$.*

Demostración. La demostración es inmediata por la definición. Los dos isomorfismos se obtienen del Teorema de Isomorfía. El inducido por f porque $Ker(f) = (0)$ y $M'/(0) = M' \Rightarrow M'/Ker(f) \cong f(M')$. El inducido por g porque $Im(g) = M''$ y $f(M') = Im(f) = Ker(g) \Rightarrow M/f(M') \cong M''$.

□

Proposición 1.4.1. *Dada una sucesión de A-módulos y homomorfismos*

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

esta es exacta si y sólo si, para cualquier A-módulo N, la sucesión

$$0 \to Hom(M'', N) \xrightarrow{g^*} Hom(M, N) \xrightarrow{f^*} Hom(M', N)$$

es exacta.

Demostración.

- $\Leftarrow$
  Supongamos la sucesión $0 \to Hom(M'', N) \xrightarrow{g^*} Hom(M, N) \xrightarrow{f^*} Hom(M', N)$ exacta para todo N. Como g^* es inyectiva, entonces g es sobreyectiva. Además, la composición $f^* \circ g^* = 0$ y para cualquier homomorfismo $v : M'' \to N$ se tiene $g \circ f \circ v = 0$. Tomando $N = M''$ y v la aplicación identidad, se tiene $g \circ f = 0$ de donde $Im(f) \subseteq Ker(g)$. Ahora, tomando $N = M/Im(f)$ y sea $\varphi : M \to N$ la proyección, $\varphi \in Ker(f^*)$, existe un homomorfismo $\psi : M'' \to N$ tal que $\varphi = \psi \circ g = g^*(\psi)$. De aquí, $Im(f) = Ker(\varphi) \supseteq Ker(g)$.

- $\Rightarrow$.
  Supongamos la sucesión $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ exacta. Si $u : M'' \to N$ es un A-homomorfismo, su imagen en $Hom_A(M, N)$ se obtiene componiendo u con la aplicación g, que es sobreyectiva. Si $u \circ g = 0$, entonces $u = 0$ porque g es sobreyectiva, lo que muestra que g^* es inyectiva, es decir, $Ker(g*) = \{0\}$. Como $g \circ f = 0$, se sigue que $0 = (g \circ f)^* = f^* \circ g^*$ y entonces $Im(g^*) \subseteq Ker(f^*)$. De igual forma, al considerar un homomorfismo $v : M \to N$ tal que la composición $v \circ f = 0$, entonces v se anula en $Im(f)$. Ahora, como g es sobre, se tiene un isomorfismo

$\phi : M'' \to M/Im(f)$ y se puede factorizar u a través de M''. De este modo se ve que $Ker(f^*) \subseteq Im(g^*)$.

$\square$

Proposición 1.4.2 (Lema de escisión). *Sea una sucesión exacta de A-homomorfismos de la forma*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

las condiciones siguientes son equivalentes:

1. *Existe $s \in Hom_A(M, M')$ tal que $s \circ f = 1_{M'}$.*

2. *Existe $t \in Hom_A(M'', M)$ tal que $g \circ t = 1_{M''}$.*

3. *Existen $s \in Hom_A(M, M')$ y $t \in Hom_A(M'', M)$ tales que $s \circ f = 1_{M'}$, $g \circ t = 1_{M''}$, y $f \circ s + t \circ g = 1_M$.*

Si una de estas condiciones se cumplen, entonces

$$M = f(M') \oplus t(M'') \cong M' \oplus M''$$

Demostración.

- 1. $\Rightarrow$ 2.
Sea $h : M'' \to M/Ker(g) = M/Im(f)$ la inversa del isomorfismo inducido por g tal que $M/Ker(g) \to M''$. Esto quiere decir que la aplicación de paso al cociente $M \to M/Im(f)$ se puede escribir como $h \circ g$. Suponiendo $s \in Hom_A(M, M')$ tal que $s \circ f = 1_{M'}$, se considera el homomorfismo $\varphi = 1_M - f \circ s \in Hom_A(M, M)$.
Entonces, $\varphi \circ f = (1_M - f \circ s) \circ f = f - f = 0$. Por lo tanto, φ se factoriza via $M/Im(f)$ proporcionando un homomorfismo $\varphi' : M/Im(f) \to M$ tal que $\varphi = \varphi' \circ h \circ g$. Denotamos $t = \varphi' \circ h \in Hom_A(M'', M)$, y se tiene $t \circ g = \varphi = 1_M - f \circ s$. Entonces, $g \circ t \circ g = g - g \circ f \circ s = g - 0 = 1_{M''} \circ g$. Como g es sobreyectiva, entonces $g \circ t = 1_{M''}$.

- 2. $\Rightarrow$ 3.
Supongamos $t \in Hom_A(M'', M)$ tal que $g \circ t = 1_{M''}$ y se considera el homomorfismo $1_M - t \circ g \in Hom_A(M, M)$. Entonces se tiene que

$$g \circ (1_M - t \circ g) = g - g = 0$$

lo que implica que $Im(1_M - t \circ g) \subseteq Ker(g) = f(M')$. Sea $s \in Hom_A(M, M')$ la composión de $1_M - t \circ g$ con la inversa del isomorfismo $f : M' \to f(M')$. Entonces $f \circ s = 1_M - t \circ g$ y por tanto, $f \circ s + t \circ g = 1_M$. Esto implica que $f \circ s \circ f = f - t \circ g \circ f = f - 0 = f \circ 1_{M'}$. Como f es inyectiva, se tiene $s \circ f = 1_{M'}$.

- 3. $\Rightarrow$ 1. Inmediato.

Falta comprobar que $M = f(M') \oplus t(M'') \cong M' \oplus M''$. Si consideramos las aplicaciones $t \in Hom_A(M'', M)$ tal que $g \circ t = 1_{M''}$ y s construida como anteriormente en la demostración 2. $\Rightarrow$ 3., recordemos que $f \circ s + t \circ g = 1_M$

de donde $M = f(s(M)) + t(g(M))$ y como g es sobreyectiva y $s : f(M') \to M'$ es sobreyectiva, $M = f(M') + t(M'')$. Ahora, para ver que se trata de la suma directa supongamos dos elementos $x' \in M'$ y $x'' \in M''$ de forma que se cumple $f(x') + t(x'') = 0$ y apliquemos g a esta igualdad:

$$g(f(x')) + g(t(x'')) = g(0)$$

Como $Im(f) = Ker(g) \Rightarrow g(f(x')) = 0$ y como $g \circ t = 1_{M''} \Rightarrow g(t(x'')) = x''$ y entonces, $0 + x'' = 0 \Rightarrow x'' = 0$. De aquí, $f(x') + t(x'') = f(x') + 0 = 0$ luego $f(x') = 0$ y como f es inyectiva, $x' = 0$, luego $M = f(M') \oplus t(M'')$. Por otro lado, por el Teorema de isomorfía, como f es inyectiva $Ker(f) = 0$ y entonces $M'/Ker(f) = M' \cong f(M')$. Por último, la igualdad $g \circ t = 1_{M''}$ implica que t es inyectiva y también $t(M'') \cong M''$. Por tanto,

$$M = f(M') \oplus t(M'') \cong M' \oplus M''$$

□

Definición 1.4.2. Una sucesión exacta se llama escindida si cumple alguna de las condiciones equivalentes anteriores.

Lema 1.4.2. *La sucesión exacta* $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ *es escindida si, y sólo si, existe un submódulo* N *de* M *tal que* $M = Im(f) \oplus N$*, y en este caso,* N *es isomorfo a* M''*.*

Demostración.

- $\Rightarrow$.
  Si suponemos la sucesión exacta y escindida, entonces es claro que se tiene $M = f(M') \oplus t(M'')$, donde $t \in Hom_A(M'', M)$ y entonces $t(M'')$ es un submódulo de M isomorfo a M''.

- $\Leftarrow$.
  Ahora, suponemos que existe un submódulo N de M tal que podemos escribir M como la suma directa $M = Im(f) \oplus N$. Vamos a ver que la restricción $g|_N : N \to M''$ es un isomorfismo. Si tomamos $x \in N$ tal que $g(x) = 0$ entonces $x \in Ker(g) = Im(f)$, pero $Im(f) \cap N = 0$, luego $x = 0$ y $g|_N$ es inyectiva. Para ver que es sobreyectiva, supongamos $y \in M''$ y sabemos que existe $x \in M$ tal que $g(x) = y$ (por ser g sobreyectiva). Ahora, $M = Im(f) \oplus N$. Supongamos $x \in Im(f) = Ker(g)$ y entonces $g(x) = 0$, luego debe ser $x \in N$. Tomando $t = (g|_N)^{-1}$ se tiene $g \circ t = 1_M$ y la sucesión es, por tanto, escindida.

□

1.5. Producto Tensorial de Módulos.

Definición 1.5.1. Dado un anillo conmutativo A, consideremos M, N y T tres A-módulos. Una aplicación $f : M \times N \to T$ se dice que es A-bilineal si para cada $x \in M$ la aplicación $y \mapsto f(x, y)$ de N en T es A-lineal, y para cada $y \in N$ la aplicación $x \mapsto f(x, y)$ de M en T es A-lineal.

Teorema 1.5.1 (**Propiedad Universal del Producto Tensorial**)**.** *Sean M y N A-módulos. Entonces, existe un par (T, g) formado por un A-módulo T y una aplicación A-bilineal $g : M \times N \to T$ con la siguiente propiedad:*
Para cada A-módulo P y cualquier aplicación A-bilineal $f : M \times N \to P$, existe una aplicación A-lineal única $f' : T \to P$ tal que $f = f' \circ g$ (es decir, cada aplicación bilineal sobre $M \times N$ se factoriza a través de T).
Además, si (T, g) y (T', g') son dos pares con esta propiedad, entonces existe un isomorfismo único $j : T \longrightarrow T'$ tal que $j \circ g = g'$.

Demostración.

- Unicidad.
  Suponemos (T', g') otro par cumpliendo la propiedad Universal. Reemplazando (P, f) por (T', g') se tiene una aplicación única $j : T \to T'$ tal que $g' = j \circ g$. Ahora, intercambiando T y T' en j se tiene otra aplicación única $j' : T' \to T$ tal que $g = j' \circ g'$, y tenemos los siguiente diagramas que deben ser conmutativos.

$$
\begin{array}{ccc}
M \times N & \xrightarrow{g} & T \\
{}_g\downarrow & \overset{g'}{\searrow} & \uparrow_{j'} \\
T & \xrightarrow{j} & T'
\end{array}
\qquad
\begin{array}{ccc}
M \times N & \xrightarrow{g'} & T' \\
{}_{g'}\downarrow & \overset{g}{\searrow} & \uparrow_{j} \\
T' & \xrightarrow{j'} & T
\end{array}
$$

  En particular, para cada par (T, g) y (T', g') también se cumple la propiedad universal: existen aplicaciones únicas $k : T \to T$ y $k' : T' \to T'$ tales que $g = k \circ g$ y $g' = k' \circ g'$. La aplicación identidad cumple estas dos condiciones, y como las aplicaciones k y k' son únicas, entonces $k = 1_T$ y $k' = 1_{T'}$. Por tanto, por los diagramas, cada una de las composiciones $j \circ j'$, $j' \circ j$ debe ser la aplicación identidad, y j y j' son inversas una de la otra. Las condiciones $g' = j \circ g$ y $g = j' \circ g'$ nos dicen que el isomorfismo es único.

- Existencia.
  Dados M y N dos A-módulos. Se construye el A-submódulo libre

$$C = \{a_1(x_1, y_1) + ... + a_t(x_t, y_t) | a_i \in A, x_i \in M, y_i \in N\}.$$

  Los elementos de C son combinaciones lineales de elementos de $M \times N$ con coeficientes en A (Si $x \in M$, $y \in N$ se entiende $(x, y) \in C$ identificando (x, y) con $1(x, y)$). Sea D el submódulo generado por todos los elementos de C de los siguientes tipos:

$$
\begin{gathered}
(x_1 + x_2, y_1) - (x_1, y_1) - (x_2, y_1) \\
(x_1, y_1 + y_2) - (x_1, y_1) - (x_1, y_2) \\
(ax, y) - a(x, y) \\
(x, ay) - a(x, y)
\end{gathered}
$$

$$
\begin{aligned}
x, x_1, x_2 &\in M \\
y, y_1, y_2 &\in N \\
a &\in A
\end{aligned}
$$

Sea $T = C/D$. Para cada elemento (x, y) de la base de C, se indica por $x \otimes y$ su clase en T. Entonces, T está generado por los elementos de la forma $x \otimes y$ que por definición cumplen:

1. $(x_1 + x_2) \otimes y - (x_1 \otimes y + x_2 \otimes y) = 0$, $\forall x_1, x_2 \in M, y \in N$
2. $x \otimes (y_1 + y_2) - (x \otimes y_1 + x \otimes y_2) = 0$, $\forall x \in M, y_1, y_2 \in N$
3. $ax \otimes y = x \otimes ay = a(x \otimes y)$, $\forall x \in M, y \in N, a \in A$

La aplicación $g : M \times N \to T$ definida por $g(x, y) = x \otimes y$ es A-bilineal. Para toda aplicación f de $M \times N$ en un A-módulo P se tiene la extensión mediante linealidad en un homomorfismo de A-módulos $F : C \to P$. Supongamos en particular que f es A-bilineal. Entonces, por las definiciones de los generadores de D, $F : C \to P$ se anula en los generadores de D, y por tanto se anula en todo D, lo que induce un homomorfismo f' de $T = C/D$ en P tal que $f'(x \otimes y) = f(x, y)$(es decir, $f = f' \circ g$). Como C está generado por $M \times N$ y se tiene la aplicación sobreyectiva $C \to T$, entonces T está generado por $g(M \times N)$. Por lo tanto, un homomorfimo $T \to P$ está determinado por su restricción a $g(M \times N)$. De aquí se tiene la unicidad de f'. Este homomorfismo f' está bien definido y es el único con esta condición, lo que implica que el par (T, g) satisface las condiciones de la proposición.

$\square$

Definición 1.5.2. Se define el Producto Tensorial de M y N y se denota por $M \otimes_A N$ (si no existe confusión sobre el anillo lo denotaremos $M \otimes N$) el módulo T anterioremente construido, que está generado como A-módulo por los productos $x \otimes y$. Si $(x_i)_{i \in I}$, $(y_j)_{j \in J}$ son generadores de M y N respectivamente, $M \otimes_A N$ está generado por los elementos $\{x_i \otimes y_j\}_{i \in I, j \in J}$.

Nota.
La notación $x \otimes y$ es ambigua a menos que se especifique el producto tensorial al que pertenece. Sean M', N' dos submódulos de M y N respectivamente y tomamos $x \in M'$ e $y \in N'$. Puede suceder que $x \otimes y$ sea cero como elemento de $M \otimes N$, aunque como elemento de $M' \otimes N'$ no sea nulo. Por ejemplo, en el caso en el que $A = \mathbb{Z}$, $M = \mathbb{Z}$ y $N = \mathbb{Z}/2\mathbb{Z}$ consideramos el submódulo M' de M igual a $2\mathbb{Z}$ y $N' = N$. Sea y' el elemento no nulo de N, es decir $y' = \bar{1}$ y se considera el producto $2 \otimes y'$. Como elemento de $M \otimes N$ es cero ya que $2 \otimes y' = 1 \otimes 2y' = 1 \otimes 0 = 0$. Sin embargo, si lo consideramos como elemento de $M' \otimes N'$, no puede ser un elemento nulo ya que por el apartado 3 de la Proposición 1.5.1 que veremos más adelante, $M' \otimes N' = \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/2\mathbb{Z}$. Y si $2 \otimes y' = 0$, entonces $\mathbb{Z}/2\mathbb{Z} = \{0\}$ y es una contradicción.

Definición 1.5.3. Sea A un anillo conmutativo y $\{M_n\}_{n \geq 0}$ una familia finita de A-módulos y P otro A-módulo. Se define una aplicación A-multilineal $f : M_1 \times \cdots M_n \to P$ como una aplicación que es A-lineal para cada variable.

Teorema 1.5.2 (**Prop. Universal del Producto Tensorial de n A-módulos**). *Sean $M_1, \cdots, M_n$, $n \leq 0$ A-módulos. Entonces, existe un par (T, g) formado por un A-módulo T y una aplicación A-multilineal $g : M_1 \times \cdots \times M_n \to T$ con la siguiente propiedad:*
Para cada A-módulo P y una aplicación A-multilineal $f : M_1 \times \cdots \times M_n \to T$, existe un homomorfismo de A-módulos único $f' : T \to P$ tal que $f = f' \circ g$.
Además, si (T, g) y (T', g') son dos pares con esta propiedad, entonces existe un isomorfismo único $j : T \longrightarrow T'$ tal que $j \circ g = g'$.

Demostración. La prueba es análoga a la del Teorema anterior pero aplicada a n A-módulos.

□

Definición 1.5.4. Se define el producto tensorial de n A-módulos como el producto $T = M_1 \otimes \cdots \otimes M_n$ generado por los elementos de la forma $x_1 \otimes \cdots \otimes x_n$ cuando $x_i \in M_i$, $1 \leq i \leq n$. De forma general, para todo entero $n \geq 0$, el A-modulo Producto Tensorial de n modulos iguales que M se denota $T^n(M)$, considerando $T^1(M) = M$ y $T^0(M) = A$.

Proposición 1.5.1. *Dados un anillo conmutativo A y tres A-módulos M, N, y P, existen:*

1. *Isomorfismos de asociatividad únicos*

$$(M \otimes N) \otimes P \to M \otimes (N \otimes P) \to M \otimes N \otimes P$$

   tales que

$$(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z) \mapsto x \otimes y \otimes z$$

2. *Un isomorfismo de distributividad respecto a la suma directa*

$$(M \oplus N) \otimes P \to (M \otimes P) \oplus (N \otimes P)$$

   tal que

$$(x, y) \otimes z \mapsto (x \otimes z, y \otimes z)$$

   para $x \in M$, $y \in N$ y $z \in P$.

3. *Un isomorfismo*

$$A \otimes M \to M$$

   tal que

$$a \otimes x \mapsto ax$$

   para $a \in A$ y $x \in M$.

Demostración. 1. Veamos si las aplicaciones del enunciado están bien definidas. Se construyen los homomorfismos

$$(M \otimes N) \otimes P \xrightarrow{f} M \otimes N \otimes P \xrightarrow{g} (M \otimes N) \otimes P$$

tales que $f((x \otimes y) \otimes z) = x \otimes y \otimes z$ y $g(x \otimes y \otimes z) = (x \otimes y) \otimes z$ para $x \in M$, $y \in N$ y $z \in P$.
Para construir f, se fija el elemento $z \in P$. La aplicación $(x, y) \mapsto x \otimes y \otimes z$ es bilineal en x y en y por lo que para cada z, induce un homomorfismo $f_z : M \otimes N \to M \otimes N \otimes P$ tal que $f_z(x \otimes y) = x \otimes y \otimes z$. Ahora se considera la aplicación $(t, z) \mapsto f_z(t)$ que va de $(M \otimes N) \times P$ en $M \otimes N \otimes P$. Esta aplicación es bilineal en t y z por lo que induce un homomorfismo

$$f : (M \otimes N) \otimes P \to M \otimes N \otimes P$$

tal que $f((x \otimes y) \otimes z) = x \otimes y \otimes z$.
Para construir g, se considera la aplicación $(x, y, z) \mapsto (x \otimes y) \otimes z$ de $M \times N \times P$ en $(M \otimes N) \otimes P$. Esta aplicación es lineal en cada variable lo que induce un homomorfismo

$$g : M \otimes N \otimes P \to (M \otimes N) \otimes P$$

tal que $g(x \otimes y \otimes z) = (x \otimes y) \otimes z$. Necesariamente las composiciones $g \circ f$ y $f \circ g$ son la identidad, puesto que son la identidad en un sistema de generadores, por lo que g y f son isomorfismos.
La prueba de la segunda parte se realiza de forma análoga construyendo los homomorfismos

$$M \otimes (N \otimes P) \xrightarrow{f} M \otimes N \otimes P \xrightarrow{g} M \otimes (N \otimes P)$$

tales que $f(x \otimes (y \otimes z)) = x \otimes y \otimes z$ y $g(x \otimes y \otimes z) = x \otimes (y \otimes z)$ para $x \in M$, $y \in N$ y $z \in P$.

2. De forma similar provamos que, para $x \in M$, $y \in N$ y $z \in P$, el morfismo $(M \oplus N) \otimes P \to (M \otimes P) \oplus (N \otimes P)$ dado por $(x, y) \otimes z \mapsto (x \otimes z, y \otimes z)$ y su morfismo inverso $(M \otimes P) \oplus (N \otimes P) \to (M \oplus N) \otimes P$ que viene dado por $(x \otimes z, y \otimes z) \mapsto (x, 0) \otimes z + (0, y) \otimes z$ están bien definidos.

3. De forma similar.

$\square$

Proposición 1.5.2. *El isomorfismo de asociatividad se puede extender para familias finitas de A-módulos.*

$$(M_1 \otimes \cdots \otimes M_d) \otimes (M_{d+1} \otimes \cdots \otimes M_n) \cong M_1 \otimes \cdots \otimes M_n$$

Demostración. Solamente hace falta razonar por recurrencia sobre d y n aplicando el punto 1. de la Proposición anterior.

$\square$

1.6. Exactitud del Producto Tensorial

Dado un anillo conmutativo A y dados dos A-homomorfismos $f : M \to M'$ y $g : N \to N'$, podemos definir la aplicación bilineal $(f, g) : M \times N \to M' \otimes N'$, con $(f, g)(x, y) = f(x) \otimes f(y)$. Esta aplicación induce un A-homomorfismo

$$h : M \otimes N \to M' \otimes N'$$

dado por $h(x \otimes y) = f(x) \otimes g(y)$ para $x \in M$, $y \in N$.

Definición 1.6.1. Dado un anillo conmutativo A y dados dos A-homomorfismos $f : M \to M'$ y $g : N \to N'$. Se define el producto tensorial de f y g, y se denota por $f \otimes g$, como el A-homomorfismo h anterior: $f \otimes g : M \otimes N \to M' \otimes N'$, dado por $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$ para $x \in M$, $y \in N$.

Nota.
En las condiciones de la definción anterior, si $f' : M' \to M''$ y $g' : N' \to N''$ son otros dos A-homomorfismos, se cumple la igualdad

$$(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g)$$

ya que ambos homomorfismos coinciden en los generadores de $M \otimes N$ que son los elementos de la forma $x \otimes y$.

Teorema 1.6.1. *Dado un anillo conmutativo A y dados tres A-módulos M, N y P, existe un isomorfismo canónico*

$$Hom(M \otimes N, P) \stackrel{\sim}{\to} Hom(M, Hom(N, P))$$

Demostración. Sea $f : M \times N \to P$ una aplicación A-bilineal. Para cada $x \in M$ la aplicación $y \mapsto f(x, y)$ que va de N en P es A-lineal, luego induce una aplicación $M \to Hom(N, P)$ que es A-lineal por ser f lineal en la variable x. Ahora, dado un A-homomorfismo $g : M \to Hom(N, P)$ podemos definir una aplicación bilineal dada por $(x, y) \mapsto g(x)(y)$. Es decir, el conjunto de todas las aplicaciones A-bilineares de $M \times N$ en P está en correspondencia con $Hom(M, Hom(N, P))$. Además, por la Propiedad Universal del Producto Tensorial, también está en correspondencia con $Hom(M \otimes N, P)$. En definitiva, se tiene

$$Hom(M \otimes N, P) \stackrel{\sim}{\to} Hom(M, Hom(N, P))$$

□

Proposición 1.6.1. *Dada una sucesión exacta de A-módulos y homomorfismos $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$, y sea N otro A-módulo, entonces la sucesión*

$$M' \otimes N \xrightarrow{f \otimes 1_N} M \otimes N \xrightarrow{g \otimes 1_N} M'' \otimes N \to 0$$

es exacta.

Demostración. Por la Proposición 1.4.1, como $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ es exacta, para cualquier A-módulo P también lo es

$$0 \to Hom(M'', Hom(N,P)) \xrightarrow{g^*} Hom(M, Hom(N,P)) \xrightarrow{f^*} Hom(M', Hom(N,P))$$

Por el isomorfismo del Teorema 1.6.1, se tiene que

$$0 \to Hom(M'' \otimes N, P) \to Hom(M \otimes N, P) \to Hom(M' \otimes N, P)$$

es una sucesión exacta y volviendo a aplicar la otra implicación de la Proposición 1.4.1, tendremos que también es exacta la sucesión

$$M' \otimes N \xrightarrow{f \otimes 1_N} M \otimes N \xrightarrow{g \otimes 1_N} M'' \otimes N \to 0$$

$\square$

Corolario 1.6.1. *Dada una sucesión exacta de A-módulos y homomorfismos $M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$, y sea N otro A-módulo, entonces la sucesión*

$$N \otimes M' \xrightarrow{1_N \otimes f} N \otimes M \xrightarrow{1_N \otimes g} N \otimes M'' \to 0$$

es exacta.

Demostración. Podemos establecer un isomorfismo $h : M \otimes N \to N \otimes M$ dado por $h(x \otimes y) = y \otimes x$. Aplicando la Proposición 1.6.1 se tiene la demostración. $\square$

Proposición 1.6.2. *Sea A un anillo conmutativo. Dadas las sucesiones exactas de A-módulos:*

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

$$N' \xrightarrow{s} N \xrightarrow{t} N'' \to 0$$

el A-homomorfismo producto tensorial de g y t, $g \otimes t : M \otimes N \to M'' \otimes N''$ es sobreyectivo y su núcleo es

$$Im(f \otimes 1_N) \oplus Im(1_M \otimes s)$$

Demostración. Por la fórmula de la Nota de la Definición 1.6.1, podemos escribir $g \otimes t$ como la descomposición

$$g \otimes t = (g \circ 1_M) \otimes (1_{N''} \circ t) = (g \otimes 1_{N''}) \circ (1_M \otimes t)$$

Por la Proposición 1.6.1 y su Corolario, cada unos de los homomorfismos cuya composición es $g \otimes t$ es sobreyevtivo, luego $g \otimes t$ es sobreyectivo por ser composición de dos homomorfismos sobreyectivos.
Por otra parte, tomamos $z \in M \otimes N$ y para ver que z está en $Ker(g \otimes t)$ es necesario y suficiente que $(1_M \otimes t)(z)$ pertenezca al núcleo de $g \otimes 1_{N''}$ debido a la descomposición de $g \otimes t$. Pero por la Proposición 1.6.1 se tiene

$Ker(g \otimes 1_{N''}) = Im(f \otimes 1_{N''})$ y $f \otimes 1_{N''} : M' \otimes N'' \to M \otimes N''$, luego $z \in Ker(g \otimes 1_{N''}) \Leftrightarrow z \in Im(f \otimes 1_{N''})$. Además, como el homomorfismo $t : N \to N''$ es sobreyectivo, también es cierto para $1_{M'} \otimes t : M' \otimes N \to M' \otimes N''$. Entonces, la condición para z se reduce a la existencia de un $a \in M' \otimes N$ tal que $(1_M \otimes t)(z) = (f \otimes t)(a)$. Tomando $b = z - (f \otimes 1_N)(a)$, se tendrá

$$(1_M \otimes t)(b) = (1_M \otimes t)(z) - (1_M \otimes t) \circ (f \otimes 1_N)(a) =$$

$$= (1_M \otimes t)(z) - (f \otimes t)(a) = (1_M \otimes t)(z) - (1_M \otimes t)(z) = 0$$

y como la sucesión $M' \otimes N \xrightarrow{f \otimes 1_N} M \otimes N \xrightarrow{g \otimes 1_N} M'' \otimes N \to 0$ es exacta, b pertenece a $Im(1_M \otimes s)$.

$\square$

Proposición 1.6.3. *Dadas dos familias de A-módulos* $\{M_i\}_{i \in I}$ *y* $\{N_j\}_{j \in J}$ *de A-módulos. Existe un isomorfismo de distributividad*

$$(\bigoplus_{i \in I} M_i) \otimes (\bigoplus_{j \in J} N_j) \cong \bigoplus_{i,j} (M_i \otimes N_j)$$

Demostración. Denotando $M = \bigoplus_{i \in I} M_i$ y $N = \bigoplus_{j \in J} N_j$, veamos que la aplicación

$$g : M \otimes N \to \bigoplus_{i,j} (M_i \otimes N_j)$$

tal que para $m = \sum_{i \in I} m_i$ y $n = \sum_{j \in J} n_j$ está dada por $g(m \otimes n) = \sum_{i,j} (m_i \otimes n_j)$ es biyectiva. Para ello, sean $q_i : M_i \to M$ y $p_j : N_j \to N$ las respectivas inclusiones canónicas, se define un aplicación lineal

$$h_{i,j} : M_i \times N_j \to M \otimes N$$

dada por $h_{i,j} = q_i \otimes p_j$, y de esta se obtiene el homomorfimo

$$h : \bigoplus_{i,j} (M_i \otimes N_j) \to M \otimes N$$

$$\sum_{i,j} (m_i \otimes n_j) \longmapsto \sum_i q_i(m_i) \otimes \sum_j p_j(n_j)$$

Entonces, la composición $h \circ g$ es la aplicación identidad en los elementos que engendran el A-módulo $M \otimes N$ que son los de la forma $(\sum_{i \in I} m_i) \otimes (\sum_{j \in J} n_j)$. Y, también se tiene que la composición $g \circ h$ es la identidad para los elementos de la forma $\sum_{i,j} (m_i \otimes n_j)$, que engendran el A-módulo $\bigoplus_{i,j} (M_i \otimes N_j)$, ya que para cada (i, j), los productos $m_i \otimes n_j$ engendran los A-módulos $M_i \otimes N_j$.

$\square$

1.7. Producto Tensorial de Álgebras.

Proposición 1.7.1. *Sea A un anillo conmutativo y B un A-módulo. Entonces, proporcionar a B una estructura de A-álgebra es equivalente a proporcionar un A-homomorfismo $u : B \otimes B \to B$ satisfaciendo las siguientes condiciones:*

1. *El diagrama*

$$\begin{array}{ccc} B \otimes B \otimes B & \xrightarrow{1_B \otimes u} & B \otimes B \\ {\scriptstyle u\otimes 1_B}\downarrow & & \downarrow{\scriptstyle u} \\ B \otimes B & \xrightarrow{u} & B \end{array}$$

   es conmutativo.

2. *Existe un elemento $1 \in B$ tal que $u(1 \otimes b) = b = u(b \otimes 1)$ para todo $b \in B$.*

Demostración.

- $\Rightarrow$.
  Supongamos que B es un A-álgebra cuyo homomorfismo estructural es $\varphi : A \to B$. La aplicación $B \times B \to B$ que define la multiplicación en B es A-bilineal. De aquí obtenemos un A-homomorfismo $u : B \otimes B \to B$ dado por $u(b \otimes b') = bb'$, para $b, b' \in B$. Esta aplicación cumple las condiciones requeridas ya que de la asociatividad de la multiplicación en B, se obtiene de la condición de conmutatividad del diagrama

$$(\varphi(a)b)b' = u(\varphi(a)b \otimes b') = u(b \otimes \varphi(a)b') = b(\varphi(a)b')$$

  y, de la existencia de un elemento neutro para la multiplicación en B, se obtiene la segunda condición.

- $\Leftarrow$.
  Ahora, veamos la vuelta de la equivalencia, y dado $u : B \otimes B \to B$ como en el enunciado, se define la multiplicación en B como $bb' = u(b \otimes b')$. Esta multipllicación es asociativa por la conmutatividad del diagrama, y el elemento $1 \in B$ dado será el elemento neutro de B. La distributividad con respecto a la suma es una consecuencia de las propiedades del producto tensorial. Por tanto, B tiene estructura de anillo. Además se cumple que

$$(aa')(bb') = (aa')u(b \otimes b') = u(aa'b \otimes b') = u(ab \otimes a'b') = (ab)(a'b')$$

  para $a, a' \in A$ y $b, b' \in B$. Por lo que B también está dotado de estructura de A-álgebra.

□

Proposición 1.7.2. *Dado un anillo conmutativo A, se consideran B y C dos A-álgebras con sus respectivos homomorfismos $f : A \to B$, $g : A \to C$. Como B y C son A-módulos podemos construir su producto tensorial $D = B \otimes C$. Entonces, se puede definir una operación de multiplicación en D.*

Demostración. Consideremos la aplicación $B \times C \times B \times C \to D$ definida por

$$(b, c, b', c') \mapsto bb' \otimes cc'$$

Esta aplicación es A-multilineal, por ello induce un homomorfismo de A-módulos

$$B \otimes C \otimes B \otimes C \to D$$

y por el isomorfismo de asociatividad, un homomorfismo de A-módulos

$$D \otimes D \to D$$

que se corresponde con una aplicación A-bilineal $u : D \times D \to D$ que está bien definida por

$$u(b \otimes c, b' \otimes c') = bb' \otimes cc'$$

La aplicación u satisface las condiciones de la Proposición 1.7.1 con $1 = 1 \otimes 1$. De esta forma se obtiene una estructura de A-álgebra en D.

$\square$

Nota.
Por tanto, se ha definido una multiplicación en el producto tensorial $D = B \otimes C$ de la siguiente forma:

$$(b \otimes c)(b' \otimes c') = bb' \otimes cc'$$

y de forma general,

$$(\sum_i (b_i \otimes c_i))(\sum_j (b'_j \otimes c'_j)) = \sum_{i,j} (b_i b'_j \otimes c_i c'_j)$$

Definición 1.7.1. Se define como producto tensorial de las A-álgebras B y C al A-álgebra $D = B \otimes A$.

Corolario 1.7.1. *Sea A un anillo conmutativo y B una A-álgebra. Entonces,*

$$B \otimes A[t] \cong B[t]$$

Demostración. Como $A[t]$ es un A-módulo libre de la forma

$$A[t] = A \oplus At \oplus At^2 \oplus \dots$$

y, por la Proposición 1.6.3 el producto tensorial conmuta con las sumas directas, $B \otimes (\bigoplus_i At^i) \cong \bigoplus_i (B \otimes At^i)$. Además, aplicando el punto 3. de la Proposición 1.5.1, se tiene el isomorfismo $B \otimes At^i \cong Bt^i$. Es decir, por el morfismo dado por $b \otimes \sum_i a_i t^i \mapsto \sum_i a_i b t^i$ para $b \in B$, $a_i \in A$, se muestra que

$$B \otimes A[t] \cong B[t]$$

$\square$

Capítulo 2

Álgebra Tensorial y Simétrica

2.1. Álgebra Tensorial.

Dado un anillo conmutativo A y un A-módulo M. Para un entero $n \geq 0$, denotaremos $T^n(M) = M \otimes M \otimes \cdots \otimes M$ con n factores entendiendo $T^0(M) = A$ y $T^1(M) = M$. Se denota por $T(M)$ el A-módulo suma directa $\bigoplus_{n\geq 0} T^n(M)$.

A *T(M)* se le puede dotar de una estructura de A-álgebra graduada. Para conseguir esta estructura, se considera el isomorfismo de asociatividad dado en la Proposición 1.5.2

$$m_{pq} : T^p(M) \otimes T^q(M) \xrightarrow{\sim} T^{p+q}(M)$$

definido como sigue para $t \in T^p(M)$ y $x \in T^q(M)$:

$$m_{pq}(t, x) = t \otimes x$$

Estos isomorfismos, seguidos de la inclusión $T^{p+q}(M) \hookrightarrow T(M) = \bigoplus_{n\geq 0} T^n(M)$ nos proporcionan, para todo par de enteros $p \geq 0, q \geq 0$, un A-homomorfismo $m_{pq} : T^p(M) \otimes T^q(M) \longrightarrow T(M)$. Como por el isomorfismo de 1.6.3 se cumple

$$T(M) \otimes T(M) = \bigoplus_{p,q\geq 0} (T^p(M) \otimes T^q(M))$$

se tiene un A-homomorfismo

$$m : T(M) \otimes T(M) \to T(M)$$

tal que $\forall\ p, q$ se cumple $m|_{T^p(M)\otimes T^q(M)} = m_{pq}$ y este es el homomorfismo que dota a $T(M)$ con la estructura de álgebra por la Proposición 1.7.1 y será el Álgebra Tensorial del A-módulo M.

Cada elemento de $T(M)$ es una suma finita de elementos $x_1 \otimes \cdots \otimes x_n$ y la multiplicación interna y la multiplicación por un escalar se definen en los generadores por:

$$\begin{aligned} (x_1 \otimes ... \otimes x_p) \cdot (x_{p+1} \otimes ... \otimes x_{p+q}) = x_1 \otimes ... \otimes x_p \otimes x_{p+1} \otimes ... \otimes x_{p+q} \\ a \cdot (x_1 \otimes ... \otimes x_p) = (ax_1 \otimes ... \otimes x_p) \\ x_i \in M, a \in A \end{aligned}$$

y se extiende por linealidad. Es claro que la multiplicación definida sobre $T(M)$ es asociativa y tiene como elemento unidad el elemento unidad 1 de A=$T^0(M)$, pero este producto no es conmutativo. Por otra parte, hemos visto que esta álgebra descompone como $T(M) = \bigoplus_{n\geq 0} T^n(M)$ y por el producto se cumple $T^p \otimes T^q \subseteq T^{p+q}$. Por tanto, $T(M)$ es un álgebra graduada y la componente homogénea de grado n es $T^n(M)$. Sea $\varphi : M \to T(M)$ la aplicación que deriva de la aplicación de inclusión $T^1(M) = M \hookrightarrow T(M)$. Por la definición de la multiplicación en $T(M)$ se tiene

$$\varphi(x_1) \dots \varphi(x_n) = x_1 \otimes \cdots \otimes x_n$$

Por tanto, como cada elemento de $T(M)$ es una suma finita de los elementos anteriores, $T(M)$ está generado como A-álgebra por $\varphi(M) = T^1(M)$.

Definición 2.1.1. Dado un anillo conmutativo A y un A-módulo M. Se define el Álgebra Tensorial de M al par $(T(M), \varphi')$ donde $T(M)$ es el álgebra suma directa $\bigoplus_{n\geq 0} T^n(M)$ dotado de la operación de multiplicación definida anterioremente, y φ' es la aplicación inclusión $A = T^0(M) \hookrightarrow T(M)$.

Teorema 2.1.1. ***(Propiedad Universal del Álgebra Tensorial)*** *Dados A un anillo conmutativo y M un A-módulo, el par $(T(M), \varphi)$ cumple la siguiente propiedad universal:*
Sea B una A-álgebra y $f : M \to B$ una aplicación A-lineal, existe un único homomorfismo de A-álgebras $g : T(M) \to B$ tal que $f = g \circ \varphi$, donde la aplicación $\varphi : M \to T(M)$ es la inyección canónica $\varphi(M) = T^1(M)$.

Demostración. Para toda familia finita $(x_i)_{1\leq i\leq n}$ de n elementos de M, por definición del producto en $T(M)$ se tiene $x_1 \otimes x_2 \otimes ... \otimes x_n = \varphi(x_1)\varphi(x_2)...\varphi(x_n)$. Por tanto, se debe cumplir

$$g(x_1 \otimes x_2 \otimes ... \otimes x_n) = f(x_1)f(x_2)...f(x_n)$$

para $n \geq 1$ y para $a \in A$, $g(a) = a1_B$ (cuando 1_B es el elemento unidad en B) de donde se obtiene la unicidad de g.
Para probar la existencia, se tiene que para $n > 0$, la aplicación $f_n : M^n \to B$ dada por $(x_1, ..., x_n) \mapsto f(x_1)...f(x_n)$ es A-multilineal. Entonces, le corresponde un A-homomorfismo $g_n : T^n(M) \to B$ tal que

$$g_n(x_1 \otimes x_2 \otimes ... \otimes x_n) = f(x_1)f(x_2)...f(x_n)$$

Se define la aplicación estructural de B como A-álgebra $g_0 : T^0(M) \to B$ de forma que $g_0(a) = a1_B$ para todo $a \in A$. Sea g el homormorfismo de A-álgebras de $T(M)$ en B cuya restricción a $T^n(M)$ es g_n con $n \geq 0$, se tiene que $g \circ \varphi = g_1 = f$. Para probar que g es homomorfismo de A-álgebras se tiene que, por construcción $g(1) = 1_B$ y por linealidad, es suficiente probar que $g(xy) = g(x)g(y)$ si $x \in T^p(M)$, $y \in T^q(M)$ $(p > 0,\ q > 0)$. Escribiendo $x = x_1 \otimes x_2 \otimes ... \otimes x_p$ e $y = x_{p+1} \otimes x_{p+2} \otimes ... \otimes x_{p+q}$, por la definición de g_n y la multiplicación definida en el Álgebra Tensorial,

$$g(xy) = g((x_1 \otimes x_2 \otimes ... \otimes x_p) \cdot (x_{p+1} \otimes x_{p+2} \otimes ... \otimes x_{p+q}) =$$

$$= g(x_1 \otimes x_2 \otimes ... \otimes x_p \otimes x_{p+1} \otimes x_{p+2} \otimes ... \otimes x_{p+q}) =$$

$$= f(x_1) \dots f(x_p) f(x_{p+1}) \dots f(x_{p+q}) =$$

$$= (f(x_1) \dots f(x_p))(f(x_{p+1}) \dots f(x_{p+q})) =$$

$$= g(x_1 \otimes x_2 \otimes ... \otimes x_p) g(x_{p+1} \otimes x_{p+2} \otimes ... \otimes x_{p+q}) =$$

$$= g(x)g(y)$$

□

2.1.1. Propiedades funtoriales del Álgebra Tensorial.

Proposición 2.1.1. *Sea A un anillo conmutativo, M y N dos A-módulos, y $u : M \to N$ una aplicación A-lineal. Existe un homomorfismo único de A-álgebras $u' : T(M) \to T(N)$, tal que el siguiente diagrama es conmutativo:*

$$\begin{array}{ccc} M & \xrightarrow{u} & N \\ \varphi_M \downarrow & & \downarrow \varphi_N \\ T(M) & \xrightarrow{u'} & T(N) \end{array}$$

Demostración. La existencia y unicidad de u' se deducen del Teorema 2.1.1 aplicado al álgebra $T(N)$ y a la aplicación lineal $\varphi_N \circ u : M \to T(N)$.

□

Nota.
El homomorfismo u' de la proposición anterior se denotará $T(u)$.

Proposición 2.1.2. *En las condiciones de la proposición anterior. Si P es un A-módulo y $v : N \to P$ es una aplicación A-lineal, se tiene*

$$T(v \circ u) = T(v) \circ T(u)$$

Demostración. Se tienen los diagramas

$$\begin{array}{ccccccc} M & \xrightarrow{u} & N & \quad & N & \xrightarrow{v} & P \\ \varphi_M \downarrow & & \downarrow \varphi_N & & \varphi_N \downarrow & & \downarrow \varphi_P \\ T(M) & \xrightarrow{T(u)} & T(N) & & T(N) & \xrightarrow{T(v)} & T(P) \end{array}$$

y además, si $w = v \circ u$, sabemos que existe un único $w' : T(N) \to T(P)$ homomorfismo de álgebras que hace conmutativo el diagrama

$$\begin{array}{ccc} M & \xrightarrow{w} & P \\ \varphi_M \downarrow & & \downarrow \varphi_P \\ T(M) & \xrightarrow{w'} & T(P) \end{array}$$

Como la composición $T(v) \circ T(u)$ lo cumple, entonces

$$T(w) = T(v \circ u) = T(v) \circ T(u)$$

□

Nota.
Llamaremos a $T(u)$ la prolongación canónica de u en $T(M)$. La restricción $T^n(u) : T^n(M) \to T^n(N)$ es aquella tal que

$$T^n(u)(x_1 \otimes x_2 \otimes \cdots \otimes x_n) = u(x_1) \otimes u(x_2) \otimes \cdots \otimes u(x_n)$$

para $x_i \in M$ ya que $T(u)$ es un homomorfismo de álgebras y $T^1(u) = u$. La restricción $T^0(u)$ en A es la aplicación identidad.

Proposición 2.1.3. *Si $u : M \to N$ es una aplicación lineal sobreyectiva, el homomorfismo $T(u) : T(M) \to T(N)$ es sobreyectivo y su núcleo es el ideal bilateral de $T(M)$ engendrado por el núcleo $P \subset M \subset T(M)$ de u.*

Demostración. La aplicación $T^0(u) : T^0(M) \to T^0(N)$ es biyectiva. Para cualquier entero $n > 0$, la aplicación $T^n(u) : T^n(M) \to T^n(N)$ se ha definido como $T^n(u) = u \otimes u \otimes \cdots \otimes u$, n veces. Al ser u biyectiva, u induce la siguiente sucesión exacta:

$$Ker(u) \overset{i}{\hookrightarrow} M \overset{u}{\to} N \to 0$$

donde i es la inclusión, y entonces $Im(i) = Ker(u)$. De aquí, la sobreyectividad de $T^n(u)$ se obtiene por recurrencia sobre n aplicando la Proposición 1.6.2. Además, por esta misma Proposición vemos que el núcleo K_2 de la aplicación $T^2(u) = u \otimes u : M \otimes M \to N \otimes N$ es

$$Im(i \otimes 1_M) \oplus Im(1_M \otimes i) = (Ker(u) \otimes M) \oplus (M \otimes Ker(u))$$

De nuevo por recurrencia sobre n, tendremos que el núcleo K_n de cada $T^n(u)$ es el submódulo de $T^n(M)$ engendrado por los productos $x_1 \otimes x_2 \otimes \cdots \otimes x_n$ con al menos uno de los x_i perteneciente a $P = Ker(u)$. Por tanto, el núcleo $K = \oplus_{n\geq 1} K_n$ de $T(u)$ es el ideal bilatero de $T(M)$ engendrado por P.

$\square$

2.2. Álgebra Simétrica.

Sea A un anillo conmutativo y sea M un A-módulo. Se considera el ideal bilateral J generado por el conjunto $S = \{x \otimes y - y \otimes x | x, y \in M\}$ de $\mathrm{T}(M)$.

Definición 2.2.1. Sea A un anillo conmutativo y M un A-módulo. Se define el Álgebra Simétrica de M como el par $(S(M), \varphi_M)$ donde se denota por $\mathrm{S}(M)$ el álgebra sobre A que es el cociente del álgebra tensorial $\mathrm{T}(M)$ por el ideal bilateral J. Denotaremos por $\varphi_M : M \to S(M)$ a la composición $M \xrightarrow{\varphi} T(M) \to S(M)$. $S(M)$ está generado como A-álgebra por $\varphi_M(M)$.

Nota.
Como está generado por elementos homogéneos de grado 2, el ideal bilateral J es homogéneo. Denotamos $J_n = J \cap T^n(M)$. Por lo tanto, el álgebra *S(M)* es un álgebra graduada si consideramos la siguiente graduación, a la que llamaremos graduación canónica.

$$S(M) = \bigoplus_{n\geq 0} S^n(M) = \bigoplus_{n\geq 0} T^n(M)/J_n$$

Así, $J_0 = J_1 = 0$ y, canónicamente se tiene $S^0(M) = A$ y $S^1(M) = T^1(M) = M$.

De igual manera, se tiene una propiedad universal para el álgebra simétrica.

Teorema 2.2.1. ***(Propiedad Universal del Álgebra Simétrica)*** *El álgebra simétrica S(M) es una A-álgebra conmutativa y el par (S(M), φ_M) cumple la siguiente propiedad universal:*
Para todo par (B,f) donde B es una A-álgebra conmutativa y $f : M \longrightarrow B$ un homomorfismo de A-módulos, existe un único homomorfismo de A-álgebras $h : S(M) \longrightarrow B$ tal que $f = h \circ \varphi_M$.

Demostración. Como $x \otimes y - y \otimes x \in J$, por definición se tiene

$$\varphi_M(x)\varphi_M(y) = \varphi_M(y)\varphi_M(x)$$

para todo x, y $\in$ *M*. Por lo tanto, la propiedad de conmutatividad de la multiplicación en $\mathrm{S}(M)$ se deduce del hecho de que $\mathrm{S}(M)$ está generada como A-álgebra por $\varphi_M(M)$. La unicidad de h es de nuevo derivada de este mismo hecho.
Para probar la existencia de h tomaremos el homomorfismo de A-álgebras $g_1 : T(M) \longrightarrow B$ que existe por el Teorema 2.1.1 tal que $f = g_1 \circ \varphi$. Por lo que faltaría ver que g_1 se anula en el ideal J. Si

$$p : T(M) \to S(M) = T(M)/J$$

es el homomorfismo canónico, entonces $g_1 = h \circ p$ dónde $h : S(M) \to B$ es un homomorfismo de álgebras. Entonces,

$$g_1(x \otimes y - y \otimes x) = g_1(xy - yx) = g_1(x)g_1(y) - g_1(y)g_1(x) = 0$$

porque B es conmutativa. Finalmente, $g_1(J)$=0.

□

Nota.

1. En el caso en el que B sea una A-álgera graduada cuya graduación sea $B = \bigoplus_{n \geq 0} B_n$ y suponemos además que la aplicación lineal f que cumple $f(x)f(y) = f(y)f(x)$ es tal que

$$f(M) \subset B_1$$

Por la relación $h(x_1 x_2 \dots x_p) = f(x_1)f(x_2)\dots f(x_p)$ para $x_i \in M$ se tiene que $h(S^p(M)) \subset B_p$.

2. Los elementos de $S(M)$ son sumas de productos de la forma $x_1 x_2 \dots x_n$, con $x_i \in M$ donde identificamos la clase de $x_1 \otimes x_2 \otimes \dots \otimes x_n$ en $S^n(M)$ por $x_1 x_2 \dots x_n$, y por $\cdot$ la multiplicación en $S(M)$.

2.2.1. Propiedades funtoriales del Álgebra Simétrica.

Proposición 2.2.1. *Sea A un anillo conmutativo, M y N dos A-módulos, y $u : M \to N$ una aplicación A-lineal. Existe un homomorfismo único de A-álgebras $u' : S(M) \to S(N)$, tal que el siguiente diagrama es conmutativo:*

$$\begin{array}{ccc} M & \xrightarrow{u} & N \\ \varphi_M \downarrow & & \downarrow \varphi_N \\ S(M) & \xrightarrow{u'} & S(N) \end{array}$$

Además, u' es homomorfismo de álgebras graduadas.

Demostración. La existencia y unicidad de u' se deducen de Teorema 2.2.1 aplicado al álgebra conmutativa $S(N)$ y a $f = \varphi_N \circ u : M \to S(N)$.
Como $f(M) \subset S^1(N)$, de la relacción $u'(x_1 x_2 ... x_t) = f(x_1)f(x_2)...f(x_t)$ para $x_i \in M$ se deduce el hecho de que u' sea un homormorfismo de álgebras graduadas.

□

Nota.
El homomorfismo u' de la proposición anterior se denotará $S(u)$.

Proposición 2.2.2. *En las condiciones de la proposición anterior. Si P es un A-módulo y $v : N \to P$ es una aplicación A-lineal, se tiene*

$$S(v \circ u) = S(v) \circ S(u)$$

Demostración. Razonando de igual forma que en la demostración de la Proposición 2.1.2 se llega a que el único homomorfismo de álgebras que hace conmutativo el diagrama

$$\begin{array}{ccc} M & \stackrel{v\circ u}{\longrightarrow} & P \\ \varphi_M \downarrow & & \downarrow\varphi_P \\ S(M) & \stackrel{S(v\circ u)}{\longrightarrow} & S(P) \end{array}$$

es la composición $S(v) \circ S(u)$.

□

Nota.
Como $S(M)$ contiene a $M = S^1(M)$, llamaremos a $S(u)$ la prolongación canónica de u en $S(M)$. La restricción $S^n(u) : S^n(M) \to S^n(N)$ es aquella tal que

$$S^n(u)(x_1 x_2 \dots x_n) = u(x_1)u(x_2)\dots u(x_n)$$

para $x_i \in M$ ya que $S(u)$ es un homomorfismo de álgebras y $S^1(u) = u$. La restricción $S^0(u)$ en A es la aplicación identidad.

Proposición 2.2.3. *Si $u : M \to N$ es una aplicación lineal sobreyectiva, el homomorfismo $S(u) : S(M) \to S(N)$ es sobreyectivo y su núcleo es el ideal de $S(M)$ engendrado por el núcleo $P \subset M \subset S(M)$ de u, es decir, $\langle P \rangle$.*

Demostración. Se tiene la aplicación $T(u) : T(M) \to T(N)$ y que es sobreyectiva por la Proposición 2.1.3. Entonces, si J_M y J_N son los ideales bilaterales de $T(M)$ y $T(N)$ respectivamente tales que $S(M) = T(M)/J_M$ y $S(N) = T(N)/J_N$, se tiene que $T(u)(J_M) = J_N$. Si $R = Ker(T(u))$, al calcular la imagen inversa de J_N por $T(u)$, $T(u)^{-1}(J_N) = J_M + R$. Ahora bien, la aplicación $S(u) : T(M)/J_M \to T(N)/J_N$ se obtiene del paso al cociente de $T(u)$, luego es un homomorfismo sobreyectivo cuyo núcleo es $R' = (J_M + R)/J_M$. Como $R = \langle P \rangle$, R' también está generado por P.

□

Proposición 2.2.4. *Dado un A-módulo M y un A-submódulo N de este, se cumple*

$$S(M/N) = S(M)/\langle N \rangle$$

donde $\langle N \rangle$ es el $S(M)$-submódulo generado por $N \subset S(M)$, es decir, donde $\langle N \rangle = NS(M)$.

Demostración. Como la sucesión

$$0 \to N \xrightarrow{i} M \xrightarrow{u} M/N \to 0$$

es exacta, la aplicación $u : M \to M/N$ es sobreyectiva y se tiene que su núcleo será $Ker(u) = N$. Aplicando directamente la Proposición 2.2.3, se tiene que el homomorfismo $S(u) : S(M) \to S(M/N)$ es sobreyectivo, y su núcleo es el ideal engendrado por $Ker(u)$, es decir, el ideal $\langle N \rangle$. Entonces, se da el isomorfismo

$$S(M/N) \cong S(M)/Ker(S(u)) = S(M)/\langle N \rangle$$

□

2.2.2. Álgebra Simétrica de una suma directa.

Es interesante comentar el caso del Álgebra Simétrica de una suma directa.

Proposición 2.2.5. *Dado un anillo conmutativo A y dos A-módulos M_1 y M_2, existe un isomorfismo*

$$S(M_1 \oplus M_2) \xrightarrow{\sim} S(M_1) \otimes S(M_2)$$

Demostración. Sea $\varphi_i = \varphi_{M_i} : M_i \to S(M_i)$, $i = 1, 2$ y denotamos por φ a la aplicación $\varphi = \varphi_{M_1 \oplus M_2} : (M_1 \oplus M_2) \to S(M_1 \oplus M_2)$. Definimos la aplicación

$$f : (M_1 \oplus M_2) \to S(M_1) \otimes S(M_2)$$

$$f(x + y) = \varphi_1(x) \otimes 1 + 1 \otimes \varphi_2(y)$$

para $x \in M_1$, $y \in M_2$. Sean $x, x' \in M_1$, $y, y' \in M_2$, veamos que f es un A-homomorfismo:

$$f((x+y)+(x'+y')) = f((x+x')+(y+y')) = \varphi_1(x+x')\otimes 1+1\otimes\varphi_2(y+y') =$$

$$= \varphi_1(x) \otimes 1 + \varphi_1(x') \otimes 1 + 1 \otimes \varphi_2(y) + 1 \otimes \varphi_2(y') =$$

$$= \varphi_1(x) \otimes 1 + 1 \otimes \varphi_2(y) + \varphi_1(x') \otimes 1 + 1 \otimes \varphi_2(y') = f(x + y) + f(x' + y')$$

y para $a \in A$,

$$f(a(x + y)) = f(ax + ay) = \varphi_1(ax) \otimes 1 + 1 \otimes \varphi_2(ay) =$$

$$= a\varphi_1(x) \otimes 1 + 1 \otimes a\varphi_2(y) = a(\varphi_1(x) \otimes 1) + a(1 \otimes \varphi_2(y)) =$$

$$= af(x + y)$$

Por tanto, por la Propiedad Universal del álgebra simétrica $S(M_1 \oplus M_2)$, existe un homomorfismo de A-álgebras $g : S(M_1 \oplus M_2) \to S(M_1) \otimes S(M_2)$ tal que $f = g \circ \varphi$.
Por otra parte, se tiene la inclusión canónica $M_i \hookrightarrow M_1 \oplus M_2$ que induce un homomorfismo de A-álgebras $h_i : S(M_i) \to S(M_1 \oplus M_2)$, $i = 1, 2$. Se puede definir una aplicación bilineal $h : S(M_1) \times S(M_2) \to S(M_1 \oplus M_2)$ dado por

$h(a,b) = h_1(a)h_2(b)$ y por la Propiedad Universal del producto tensorial de álgebras, se tiene un homomorfismo de A-álgebras

$$h : S(M_1) \otimes S(M_2) \to S(M_1 \oplus M_2)$$

$$h(a \otimes b) = h_1(a)h_2(b)$$

para $a \in S(M_1)$ y $b \in S(M_2)$. Las composiciones $g \circ h$ y $h \circ g$ son la identidad, por lo que g es un isomorfismo.

□

Corolario 2.2.1. *Sea A un anillo conmutativo. Si M es un A-módulo libre de rango r entonces $S(M)$ es el álgebra de polinomios en r variables sobre A. Concretamente, si M es un módulo libre con base $(e_1, \ldots, e_r)$ entonces el A-morfismo $f : A[X_1, \ldots, X_r] \to S(M)$ dado por $f(X_i) = e_i$ para $1 \leq i \leq r$ es un isomorfismo de álgebras graduadas.*

Demostración. Como M es libre con base $(e_1, \ldots, e_r)$, se tiene un A-homomorfismo $g : M \to A[X_1, \ldots, X_r]$ tal que $g(e_i) = X_i$ para $1 \leq i \leq r$. Por la propiedad universal de $S(M)$, el A-homomorfismo g induce un homomorfismo de A-álgebras $h : S(M) \to A[X_1, \ldots, X_r]$. Ambos homomorfismos h y f son graduados. Además, su composición es la identidad en los generadores, luego f es un isomorfismo.

□

Capítulo 3

Teorema de Poincaré

En este capítulo se presentará el Teorema de Gauss-Bonnet, uno de los resultados principales de la Geometría Diferencial de superficies, y una de sus aplicaciones más importantes, el Teorema de Poincaré. Veremos como se relacionan el concepto geométrico de la Curvatura de Gauss y la característica de Euler, un invariante topológico de superficies. Como consecuencia de este último teorema, obtendremos un interesante resultado: Ninguna superficie homeomorfa a $\mathbb{S}^2$ puede tener un campo de vectores diferenciable sin puntos singulares. Este resultado es conocido como "Teorema de la Bola Peluda".

3.1. Nociones Previas.

Comenzaremos con algunas definiciones y resultados, que presentaremos sin demostraciones, vistos en la materia del "Grado en Matemáticas", que necesitaremos recordar para poder desarrollar la teoría de las secciones 3.2 y 3.3. Se utilizarán conceptos de la asignatura "Geometría de Curvas y Superficies" y "Análisis Matemático". Además, se seguirá la notación y definiciones de [5].

Definición 3.1.1. Un subconjunto $S \in \mathbb{R}^3$ es una superficie regular si para cada $p \in S$ existe un abierto V en $\mathbb{R}^3$ con $p \in V$ y una aplicación, que llamaremos parametrización de S,

$$x : U \to V \cap S$$

donde U es un abierto de $\mathbb{R}^2$ tales que:

1. x es diferenciable.
2. x es homeomorfismo.
3. $\forall q \in U$, la diferencial $d_x|_q : \mathbb{R}^2 \to \mathbb{R}^3$ es inyectiva. Esta condición de regularidad equivale a decir que $x_u(q)$ y $x_v(q)$ son linealmente independientes.

Definición 3.1.2. Sea $p \in S \subset \mathbb{R}^3$, con S superficie regular. Un vector tangente a S en p es un vector $v \in \mathbb{R}^3$ tal que existe una curva parametrizada de S de la forma $c : (-\varepsilon, \varepsilon) \to S$ con $c(0) = p$ y $c'(0) = v$. Al conjunto de todos los vectores tangentes a S en el punto p se le denomina plano tangente a S en p y se le representa por $T_pS \subset \mathbb{R}^3$.

Definición 3.1.3. Dado un punto p de una superficie regular $S \subset \mathbb{R}^3$. Llamaremos recta normal a S en p a la recta que pasa por p y es perpendicular al plano tangente T_pS. Llamaremos vector normal a S en p a cualquier vector unitario que genere la recta vectorial $(T_pS)^{\perp}$. Denotaremos por N_p al vector unitario normal a S en p de la forma:

$$N_p = \frac{x_u(u_0, v_0) \wedge x_v(u_0, v_0)}{||x_u(u_0, v_0) \wedge x_v(u_0, v_0)||}$$

donde x es una parametrización con $p \in x(U)$ tal que $p = x(u_0, v_0)$.

Definición 3.1.4. Sea $S \subset \mathbb{R}^3$ una superficie regular y $p \in S$. Llamamos primera forma fundamental de S en p y la representamos por I_p, a la forma bilineal que la métrica usual de $\mathbb{R}^3$ induce en el espacio vectorial T_pS:

$$I_p : T_pS \times T_pS \to \mathbb{R}$$

$$(u, v) \mapsto I_p(u, v) =< u, v >$$

Nota.
Dada una paremetrización $x : U \to S$ tal que $p \in x(U)$ con $p = x(u, , v)$, una base de T_pS viene dada por $\{x_u(u, v), x_v(u, v)\}$. En esta base, la matriz de la forma bilineal es

$$\begin{pmatrix} E & F \\ F & G \end{pmatrix}$$

con

$$E(u, v) =< x_u, x_u >= ||x_u||^2$$

$$F(u, v) =< x_u, x_v >$$

$$G(u, v) =< x_v, x_v >= ||x_v||^2$$

Definición 3.1.5. Diremos que una parametrización $x : U \to S$ de una superficie regular $S \subset \mathbb{R}^3$ es ortogonal si el ángulo que forman las rectas coordenadas en todo punto es recto.

Nota.
Como para $p = x(u_0, v_0)$ el ángulo viene dado por $cos(\varphi) = \frac{F(u_0,v_0)}{\sqrt{E(u_0,v_0)}}$ con $\varphi \in [0, \pi]$, x es ortogonal si y solo si $F \equiv 0$.

Ejemplo.
Consideramos la esfera de radio 1 y centrada en el origen en $\mathbb{R}^3$,

$$\mathbb{S}^2 = \{(x, y, z) \in \mathbb{R}^3 / x^2 + y^2 + z^2 = 1\}$$

Podemos dar una parametrización de la esfera de la siguiente forma:

$$x : (0, \pi) \times (0, 2\pi) \to \mathbb{S}^2$$

$$x(u, v) = (sin(u)cos(v), sin(u)sin(v), cos(u))$$

Entonces,

$$x_u(u, v) = (cos(u)cos(v), cos(u)sin(v), -sin(u))$$

$$x_v(u, v) = (-sin(u)sin(v), sin(v)cos(v), 0)$$

El plano tangente en el punto $p = (0, 0, 1) \in \mathbb{S}^2$ a la esfera es

$$T_p\mathbb{S}^2 = \{(x, y, z) \in \mathbb{R}^3 / z = 0\}$$

visto como plano vectorial. En la parametrización x, las entradas de la matriz de la primera forma fundamental son $E = 1$, $F = 0$, $G = sin(u)^2$, luego la parametrización x es ortogonal.

Definición 3.1.6. Llamaremos superficie orientada a una superficie regular orientable $S \subset \mathbb{R}^3$ junto con un campo de vectores diferenciable $N : S \to \mathbb{R}^3$ que es normal y unitario al que llamaremos orientación de S.

Definición 3.1.7. Sea $S \subset \mathbb{R}^3$ una superficie regular orientada (con un campo de vectores diferenciable $N : S \to \mathbb{R}^3$ normal y unitario) y sea la aplicación $A_p : T_pS \to T_pS$ el endomorfismo de Weingarten (recordemos,$A_p = -dN|_p$ donde N es la aplicación de Gauss de la superficie S). Llamamos segunda forma fundamental de S en p a la forma bilineal dada por

$$II_p(u, v) = I_p(A_p(u), v)$$

Nota.
La matriz de la segunda forma fundamental en la base $\{x_u(u_0, v_0), x_v(u_0, v_0)\}$ de T_pS viene dada por

$$\begin{pmatrix} e & f \\ f & g \end{pmatrix}$$

con

$$e(u_0, v_0) = II_p(x_u(u_0, v_0), x_u(u_0, v_0)) = \frac{|x_u, x_v, x_{uu}|}{\sqrt{EG - F^2}}$$

$$f(u_0, v_0) = II_p(x_u(u_0, v_0), x_v(u_0, v_0)) = \frac{|x_u, x_v, x_{uv}|}{\sqrt{EG - F^2}}$$

$$g(u_0, v_0) = II_p(x_v(u_0, v_0), x_v(u_0, v_0)) = \frac{|x_u, x_v, x_{vv}|}{\sqrt{EG - F^2}}$$

Definición 3.1.8. Se define por curvatura normal de $S \subset \mathbb{R}^3$ en p en la dirección de v al valor

$$k_n(v,p) = II_p(v,v) =< -dN|_p(v), v >$$

La curvatura normal máxima k_1 y la curvatura normal mínima k_2 se denominan curvaturas principales.

Definición 3.1.9. Sea $S \subset \mathbb{R}^3$ una superficie regular orientada con un campo de vectores normal N. Se denomina curvatura de Gauss de S en el punto p al valor

$$K(p) = det(A_p) = k_1(p)k_2(p)$$

Nota.
Podemos dar la curvatura de Gauss de la superficie S en el punto p en función de la parametrización relaccionándola con los coeficientes de las matrices de las formas fundamentales:

$$K(p) = \frac{eg - f^2}{EG - F^2}$$

Definición 3.1.10. Sea $S \subset \mathbb{R}^3$ una superficie regular y orientada con aplicación normal N y sea $x : U \to S$ una parametrización positivamente orientada. Definimos como símbolos de Christofell de la parametrización a las funciones diferenciables $\Gamma_{ij}^k : U \to \mathbb{R}$, $i, j, k = 1, 2$, $\Gamma_{12}^k = \Gamma_{21}^k$, tales que se cumplen las siguientes igualdades.

$$x_{uu} = \Gamma_{11}^1 x_u + \Gamma_{11}^2 x_v + eN$$

$$x_{uv} = \Gamma_{12}^1 x_u + \Gamma_{12}^2 x_v + fN$$

$$x_{vu} = \Gamma_{21}^1 x_u + \Gamma_{21}^2 x_v + fN$$

$$x_{vv} = \Gamma_{22}^1 x_u + \Gamma_{22}^2 x_v + gN$$

Nota.
Los símbolos de Christofell de la parametrización se pueden obtener a partir de los coeficientes de la primera forma fundamental y sus derivadas parciales:

$$\begin{pmatrix} \Gamma_{11}^1 & \Gamma_{12}^1 & \Gamma_{22}^1 \\ \Gamma_{11}^2 & \Gamma_{12}^2 & \Gamma_{22}^2 \end{pmatrix} = \frac{1}{EG - F^2} \begin{pmatrix} G & -F \\ -F & E \end{pmatrix} \begin{pmatrix} \frac{1}{2}E_u & \frac{1}{2}E_v & F_v - \frac{1}{2}G_u \\ F_u - \frac{1}{2}E_v & \frac{1}{2}G_u & \frac{1}{2}G_u \end{pmatrix}$$

De estas igualdades se obtiene la conocida como Fórmula de Gauss:

$$\Gamma_{11}^1\Gamma_{12}^2 + (\Gamma_{11}^2)_v + \Gamma_{11}^2\Gamma_{22}^2 - \Gamma_{12}^1\Gamma_{11}^2 - (\Gamma_{12}^2)_u - \Gamma_{12}^2\Gamma_{12}^2 = EK$$

Definición 3.1.11. Una curva en una superficie $S \subset \mathbb{R}^3$ con parametrización $\alpha : I \subset \mathbb{R} \to S \subset \mathbb{R}^3$ se denomina curva geodésica si el vector α'' es normal a S. Si es así, $||\alpha'|| = constante$.

Definición 3.1.12. Llamaremos curvatura geodésica de una curva regular parametrizada por $\alpha(s)$ en $p \in S$ al valor

$$k_g(s) = |\frac{D\alpha'(s)}{ds}|$$

que representa la variación en el cambio del ángulo que la tangente a la curva forma con una dirección paralela a través de la curva.

Nota.
Las curvas geodésicas están caracterizadas por tener curvatura geodésica igual a cero.
En el caso en el que la parametrización elegida sea ortogonal ($F = 0$), podemos expresar la curvatura geodésica en función de los coeficientes de la primera forma fundamental y sus derivadas:

$$k_g(s) = \frac{1}{2\sqrt{EG}}\{G_u\frac{dv}{ds} - E_v\frac{du}{ds}\} + \frac{d\varphi}{ds}$$

donde $\varphi(t)$ es el ángulo orientado de x_u en α'.

3.2. Teorema de Gauss-Bonnet.

Definición 3.2.1. Sea $[0, l] \subset \mathbb{R}$ y una superficie regular $S \subset \mathbb{R}^n$. Se define como curva paramétrica, cerrada, simple y regular a trozos a una aplicación continua $\alpha : [0, l] \to S$ cumpliendo

1. $\alpha(0) = \alpha(l)$.
2. $t_1 \neq t_2$, $t_1, t_2 \in [0, l) \Rightarrow \alpha(t_1) \neq \alpha(t_2)$.
3. Existe una partición $0 = t_0 < t_1 < \ldots < t_k < t_{k+1} = l$ de $[0, l]$ tal que α es diferenciable y regular en cada intervalo $[t_i, t_{i+1}]$, $i = 0, \ldots, k$.

Definición 3.2.2. Con la notación de la definición anterior, los puntos $\alpha(t_i)$, $i = 0, \ldots, k$ se denominarán los vértices de α. Las trazas $\alpha([t_i, t_{i+1}])$ se llaman los arcos regulares de α. Al hablar de curva cerrada regular a trozos nos referiremos a la traza $\alpha([0, l])$ de α.

Nota.
Supongamos una superficie orientada $S \in \mathbb{R}^n$ y una curva parametrizada, cerrada, simple y regular a trozos $\alpha : [0, l] \to S$. Entonces, en cada vértice $\alpha(t_i)$ podemos calcular los siguientes límites:

$$para\ t < t_i : \lim_{t \to t_i} \alpha'(t_i) = \alpha'(t_i^-) \neq 0$$

$$para\ t > t_i : \lim_{t \to t_i} \alpha'(t_i) = \alpha'(t_i^+) \neq 0$$

Por ser S una superficie orientada existe una normal unitaria diferenciable N definida sobre S que nos sirve para determinar la orientación positiva. De esta forma, diremos que una base $\{u, v\}$ de vectores tangentes a S está orientada positivamente si al calcular el determinante $|u, v, N|$ este nos sale positivo.
Sea $|\theta_i|$, $0 < |\theta_i| < \pi$, la menor determinación del ángulo de $\alpha'(t_i^-)$ a $\alpha'(t_i^+)$. Si $|\theta_i| \neq \pi$, asociamos a θ_i el signo del determinante $|\alpha'(t_i^-), \alpha'(t_i^+), N|$. Esto significa que si el vértice $\alpha(t_i)$ no es una "cúspide" (es decir, $|\theta_i| \neq \pi$), el signo de θ_i viene dado por la orientación de S.

Definición 3.2.3. En las condiciones anteriores, se conoce como ángulo exterior en el vértice $\alpha(t_i)$ al ángulo con signo θ_i, $-\pi < \theta_i < \pi$.

Presentaremos el siguiente teorema topológico cuya demostración se debe a H.Hopf.

Teorema 3.2.1 (Teorema de rotación de tangentes). *Sea $x : U \subset \mathbb{R}^2 \to S$ una parametrización compatible con la orientación de S, y supongamos que U es homeomorfo a un disco abierto del plano. Sea $\alpha : [0, l] \to x(U) \subset S$ una curva parametrizada, regular a trozos, cerrada y simple, con vértices $\alpha(t_i)$ y ángulos externos θ_i, $i = 0, \dots, k$. Se consideran las funciones diferenciables $\varphi_i : [t_i, t_{i+1}] \to \mathbb{R}$ que miden el ángulo positivo de x_u a $\alpha'(t)$ en cada $[t_i, t_{i+1}]$. Entonces,*

$$\sum_{i=0}^{k} (\varphi_i(t_{i+1}) - \varphi_i(t_i)) + \sum_{i=0}^{k} \theta_i = \pm 2\pi$$

donde el signo más o el signo menos dependen de la orientación de α.

Nota

El teorema establece que la variación total del ángulo a una dirección dada del vector tangente a α, más los saltos en los vértices, es igual a 2π.

Definición 3.2.4. Sea S una superficie orientada. Se dice que una región $R \subset S$ (unión de un conjunto abierto y conexo D con su frontera) es una región simple de S si es homeomorfa a un disco y la frontera ∂R es la traza de una curva parametrizada, regular a trozos, cerrada y simple $\alpha : I \to S$. En este caso, diremos que α está orientada positivamente si en cada uno de los arcos regulares abiertos $\alpha((s_i, s_{i+1}))$ de α se tiene que el campo de vectores $N \times \alpha$, producto vectorial de N y el vector α, apunta hacia el interior de D.

Definición 3.2.5. Sea f una función diferenciable sobre una superficie S, se denomina integral de f sobre la región $R \subset S$ a la integral (que no depende de la parametrización x elegida)

$$\iint_R f dA = \iint_{x^{-1}(R)} f(u, v) \sqrt{EG - F^2} dudv$$

donde dA es el elemento de área.

Definición 3.2.6. Se denomina curvatura integral de la región R a la integral

$$\iint_R KdA$$

donde K es la curvatura de Gauss.

Teorema 3.2.2 (**Teorema de Gauss-Green**). *Si $P(u,v)$ y $Q(u,v)$ son funciones diferenciables en una región simple $B \subset \mathbb{R}^2$, cuyo borde está dado por $u = u(s)$, $v = v(s)$, entonces,*

$$\sum_{i=0}^{k} \int_{s_i}^{s_{i+1}} (P\frac{du}{ds} + Q\frac{dv}{ds})ds = \iint_B (\frac{\partial Q}{\partial u} - \frac{\partial P}{\partial v})dudv$$

Teorema 3.2.3 (**Teorema de Gauss-Bonnet (Local)**). *Sea $x : U \to S$ una parametrización ortogonal (es decir, $F = 0$) de una superficie orientada S donde $U \subset \mathbb{R}^2$ es homeomorfo a un disco abierto y x es compatible con la orientación en S. Sea $R \subset x(U)$ una región simple de S y sea $\alpha : I \to S$ una curva tal que $\partial R = \alpha(I)$. Supongamos que α tiene orientación positiva parametrizada con longitud de arco s y sean $\alpha_{s_0}, \dots, \alpha_{s_k}$ y $\theta_0, \dots, \theta_k$ los vértices y los ángulos exteriores de α respectivamente. Entonces,*

$$\sum_{i=0}^{k} \int_{s_i}^{s_{i+1}} k_g(s)ds + \iint_R KdA + \sum_{i=0}^{k} \theta_i = 2\pi$$

donde $k_g(s)$ es la curvatura geodésica de los arcos regulares de α, y K es la curvatura Gaussiana de S.

Demostración. Supongamos $u = u(s)$, $v = v(s)$ la expresión de α en la parametrización x. Al ser x una parametrización ortogonal, la curvatura geodésica viene dada por

$$k_g(s) = \frac{1}{2\sqrt{EG}}\{G_u\frac{dv}{ds} - E_v\frac{du}{ds}\} + \frac{d\varphi_i}{ds}$$

donde $\varphi_i = \varphi_i(s)$ es la función diferenciable que mide el ángulo positivo de x_u a $\alpha'(s)$ en $[s_i, s_{i+1}]$. Integrando ambos lados de la igualdad en el intervalo $[s_i, s_{i+1}]$, y sumando en $i = 0, \dots, k$ obtenemos:

$$\sum_{i=0}^{k} \int_{s_i}^{s_{i+1}} k_g(s)ds = \sum_{i=0}^{k} \int_{s_i}^{s_{i+1}} \{\frac{G_u}{2\sqrt{EG}}\frac{dv}{ds} - \frac{E_v}{2\sqrt{EG}}\frac{du}{ds}\}ds + \sum_{i=0}^{k} \int_{s_i}^{s_{i+1}} \frac{d\varphi_i}{ds}ds$$

Aplicando el Teorema de Gauss-Green para $P = -\frac{E_v}{2\sqrt{EG}}$ y $Q = \frac{G_u}{2\sqrt{EG}}$ se tiene que:

$$\sum_{i=0}^{k} \int_{s_i}^{s_{i+1}} k_g(s)ds = \iint_{x^{-1}(R)} \{(\frac{E_v}{2\sqrt{EG}})_v + (\frac{G_u}{2\sqrt{EG}})_u\}dudv + \sum_{i=0}^{k} \int_{s_i}^{s_{i+1}} \frac{d\varphi_i}{ds}ds$$

Como la parametrización es ortogonal, de la fórmula de Gauss para $F = 0$ deducimos que

$$K = -\frac{1}{2\sqrt{EG}}\{(\frac{E_v}{\sqrt{EG}})_v + (\frac{G_u}{\sqrt{EG}})_u\}$$

Entonces, al sustituir,

$$\iint_{x^1(R)}\{(\frac{E_v}{2\sqrt{EG}})_v+(\frac{G_u}{2\sqrt{EG}})_u\}dudv = -\iint_{x^{-1}(R)} K\sqrt{EG}dudv = -\iint_R KdA$$

Por otra parte, en virtud del Teorema de rotación de tangentes,

$$\sum_{i=0}^{k}\int_{s_i}^{s_{i+1}}\frac{d\varphi_i}{ds}ds = \sum_{i=0}^{k}(\varphi_i(s_{i+1}) - \varphi_i(s_i)) = \pm 2\pi - \sum_{i=0}^{k}\theta_i$$

Al estar la curva α orientada positivamente, debe tomarse el signo más. Reuniendo todos los resultados anteriores se tiene que

$$\sum_{i=0}^{k}\int_{s_i}^{s_{i+1}} k_g(s)ds + \iint_R KdA + \sum_{i=0}^{k}\theta_i = 2\pi$$

$\square$

Definición 3.2.7. Sea S una superficie regular. Se dice que una región $R \subset S$ es regular en $\mathbb{R}^3$ si R es compacta y su frontera ∂R es la unión de un número finito de curvas regulares a trozos, cerradas y simples que no se cortan.

Definición 3.2.8. Llamaremos triángulo a una región simple con sólo tres vértices, y ángulos exteriores α_i, $i = 1, 2, 3$.

Definición 3.2.9. Una triangulación T de una región regular $R \subset S$ es una familia finita de triángulos T_i, $i = 1, 2, \ldots, n$ tal que

1. $\underset{i=1}{\cup}{}^n T_i = R$.
2. Si $T_i \cap T_j \neq \Phi$, entonces o bien $T_i \cap T_j$ es un lado común a T_i y a T_j, o bien consta de un vértice común a T_i y a T_j.

Dada una región regular $R \subset S$ de una superficie S, supondremos una triangulación T de R y denotaremos por F al número de triángulos, por E al número de lados y por V al número de vértices de la triangulación.

Definición 3.2.10. Se denominará característica de Euler-Poincaré de la triangulación T al número χ dado por

$$\chi = F - E + V$$

Proposición 3.2.1. *Toda región regular de una superficie regular admite una triangulación.*

Demostración. La demostración se puede encontrar en L.Ahlfors y L. Sario, *Riemann Surfaces*, Princeton University Press, Princeton.

□

Proposición 3.2.2. *Dadas una superficie orientada S y un conjunto de parametrizaciones $\{x_\lambda\}_{\lambda \in L}$ compatibles con la orientación de S y se considera una región regular $R \subset S$. Entonces, existe una triangulación T de R tal que cada triangulo $t \in T$ está contenido en algún entorno coordenado de la familia $\{x_\lambda\}_{\lambda \in L}$.*
Si además consideramos la frontera de cada triángulo $t \in T$ orientada positivamente como en la figura, en el lado común de triángulos que sean adyacentes las orientaciones serán opuestas.

Figura 3.1: Orientaciones en triángulos adyacentes

Demostración. La demostración se puede encontrar en L.Ahlfors y L. Sario, *Riemann Surfaces*, Princeton University Press, Princeton.

□

Proposición 3.2.3. *Sea $R \subset S$ una región regular de una superficie S, la característica de Euler-Poincaré no depende de la triangulación.*

Demostración. La demostración se puede encontrar en L.Ahlfors y L. Sario, *Riemann Surfaces*, Princeton University Press, Princeton.

□

Nota.
La proposición anterior muestra que χ es un invariante topológico de la región regular R. Por ello, la denotaremos $\chi(R)$.

Ejemplos.

1. Veamos que la característica de Euler de la esfera es 2. Con la triángulación considerada en la figura 3.2:

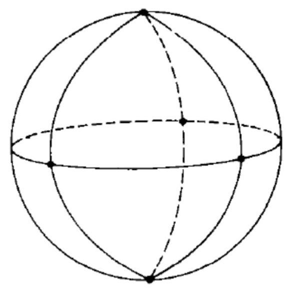


Figura 3.2: Triangulación de la esfera.

el número de triángulos es $F = 8$, el número de lados es $E = 12$ y el número de vértices es $V = 6$. Por tanto,

$$\chi(\mathbb{S}^2) = 8 - 12 + 6 = 2$$

2. La característica de Euler del toro es 0. Considerando la triángulación 3.3 en la que vemos el toro como una superficie homeomorfa a un rectángulo con sus lados correspondientes tenemos que:

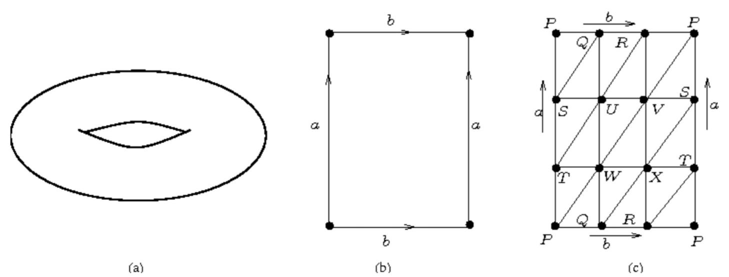


Figura 3.3: Triangulación del toro.

el número de triángulos es $F = 18$, el número de lados es $E = 21$ y el número de vértices es $V = 7$. Por tanto,

$$\chi(\mathbb{T}^2) = 18 - 21 + 7 = 0$$

3. En general, la característica del n-toro (esfera de n asas) es $-2(n-1)$.

Proposición 3.2.4 (**Clasificación de superficies compactas de** $\mathbb{R}^3$)**.** *Dada una superficie $S \subset \mathbb{R}^3$ compacta y conexa, entonces la característica de Euler-Poincaré toma uno de los siguientes valores:*

$$2, 0, -2, ..., -2n, ...$$

Además, si $S' \subset \mathbb{R}^3$ es otra superficie compacta tal que $\chi(S) = \chi(S')$, entoces S es homeomorfa a S'.

Demostración. La demostración se puede encontrar en L.Ahlfors y L. Sario, *Riemann Surfaces*, Princeton University Press, Princeton. □

Nota.
En otras palabras, cada superficie compacta y conexa S en $\mathbb{R}^3$ es homeomorfa a la esfera con un número g de agujeros. La Característica de Euler de S se relacciona con el número g de "asas" que tiene la superficie de la siguiente forma:

$$\chi(S) = -2(g-1) = 2-2g$$

Definición 3.2.11. *Denominaremos género de una superficie compacta $S \subset \mathbb{R}^3$ homeomorfa a una esfera con un número g de asas al número*

$$g = \frac{2-\chi(S)}{2}$$

Teorema 3.2.4 (**Teorema de Gauss-Bonnet(para regiones regulares).** *Sea $R \subset S$ una región regular de una superficie orientada S y sean $C_1, \ldots, C_n$ las curvas cerradas, simples y regulares a trozos que forman el borde ∂R de R. Supongamos que cada C_i tiene orientación positiva y sean $\theta_1, \ldots, \theta_p$ el conjunto de todos los ángulos exteriores de las curvas $C_1, \ldots, C_n$. Entonces,*

$$\sum_{i=1}^{n} \int_{C_i} k_g(s)ds + \iint_R KdA + \sum_{j=1}^{p} \theta_j = 2\pi\chi(R)$$

donde s denota la longitud de arco de C_i, k_g la curvatura geodésica de ∂R y la integral sobre C_i se refiere a la suma de las integrales en cada arco regular de C_i.

Demostración. Se considera una triangulación T de la región R de forma que cada triángulo T_j, $1 \leq j \leq F$, esté contenido en un entorno coordenado de una familia de parametrizaciones ortogonales, compatibles con la orientación de S que sabemos que existe por la proposición 3.2.2. Ahora, podemos aplicar la versión local del Teorema de Gauss-Bonnet a cada triángulo de $T_j \in T$ cuyos ángulos exteriores serán $\theta_{j1}, \theta_{j2}, \theta_{j3}$.

$$\int_{C_i} k_{ig}(s)ds + \iint_{T_i} KdA + \sum_{k=1}^{3} \theta_{jk} = 2\pi$$

donde k_{ig} es la curvatura geodésica de C_i. Como los triángulos adyacentes determinan orientaciones opuestas en el lado común, al sumar, las integrales que corresponden a lados que están contenides en R se cancelarán dos a dos y sólo quedarán las integrales sobre los lados que cubran ∂R. Por tanto, al sumar todos los resultados se obtiene

$$\sum_{i}^{n} \int_{C_i} k_{ig}(s)ds + \iint_R KdA + \sum_{j=1}^{F}\sum_{k=1}^{3} \theta_{jk} = 2\pi F$$

Denominaremos ángulos interiores del triángulo T_j a los dados por $\varphi_{jk} = \pi - \theta_{jk}$. Entonces,

$$\sum_{j,k}^{F,3} \theta_{j,k} = \sum_{j,k}^{F,3} (\pi - \varphi_{jk}) = \sum_{j,k}^{F,3} \pi - \sum_{j,k}^{F,3} \varphi_{jk} = 3F\pi - \sum_{j,k}^{F,3} \varphi_{jk}$$

Utilizaremos, a partir de ahora, la siguiente notación: el índice i en E_i, V_i se refiere a las componentes interiores de T (contenidas en R salvo a lo sumo, en el caso de los lados, por sus extremos) y el índice e en E_e, V_e a las exteriores (contenidas en ∂R). El número de lados de la triangulación T será $E = E_i + E_e$. Al estar ∂R parametrizado por un número finito de curvas simples, se tiene la igualdad $E_e = p$. Además, cada lado interior está en dos triángulos y cada lada exterior sólo en uno. Entonces, cuando multiplicamos el número de triángulos por 3 lados que tiene cada triángulo para calcular el número total de lados, estamos contando dos veces cada lado interior. Por lo tanto se cumple $3F = 2E_i + E_e$. Sustituyendo,

$$\sum_{j,k}^{F,3} \theta_{j,k} = 2\pi E_i + \pi E_e - \sum_{j,k}^{F,3} \varphi_{jk}$$

Si distinguimos los vértices externos que son vértices de alguna curva C_i (V_{ec}) de los vértices externos que introducimos al hacer la triangulación (V_{et}), entonces el número total de vértices externos será $V_e = V_{ec} + V_{et}$. Como la suma de ángulos alrededor de cada vértice interno es 2π, se tiene

$$\sum_{j,k}^{F,3} \theta_{jk} = 2\pi E_i + \pi E_e - 2\pi V_i - \pi V_{et} - \sum_{l}^{p} (\pi - \theta_l)$$

Sumando y restando πE_e, y teniendo en cuenta que por ser cada C_i una curva cerrada se tiene $E_e = V_e$,

$$\sum_{j,k}^{F,3} \varphi_{jk} = 2\pi E_i + 2\pi E_e - 2\pi V_i - \pi V_e - \pi V_{et} - \pi V_{ec} + \sum_{l}^{p} \theta_l = 2\pi E - 2\pi V + \sum_{l}^{p} \theta_l$$

Reuniendo todos los resultados obtenidos,

$$\sum_{i=1}^{n} \int_{C_i} k_g(s) ds + \iint_R K dA + \sum_{l=1}^{p} \theta_l = 2\pi(F - E + V) = 2\pi\chi(R)$$

$\square$

Presentaremos el siguiente corolario que es resultado directo del Teorema de Gauss-Bonnet si se tiene en cuenta que una superficie compacta puede considerarse como una región con borde vacio.

Corolario 3.2.1 (**Teoremas de Gauss-Bonnet para superficies compactas**). *Sea S una superficie compacta, conexa y orientable. Entonces, su curvatura integral viene dada por*

$$\iint_S K dA = 2\pi\chi(S)$$

3.3. Singularidades de campos de vectores sobre superficies.

Veamos una de las aplicaciones más interesantes de este Teorema que relaciona el concepto geométrico de campos de vectores, y la noción topológica de característica de Euler.

Definición 3.3.1. Un campo de vectores v en un abierto U de una superficie regular S es una aplicación $v : S \to \mathbb{R}^3$ que a cada punto $p \in U$ le asigna un vector $v(p) \in T_p(S)$.

Definición 3.3.2. Diremos que el campo de vectores v es diferenciable en p si, dada una parametrización $x(u, v)$ en p, las funciones $a(u, v)$ y $b(u, v)$ dadas por $v(p) = a(u, v)x_u(u, v) + b(u, v)x_v(u, v)$ son funciones diferenciables en p. Esta definición no depende de la parametrización.

Definición 3.3.3. Sea v un campo de vectores diferenciable de una superficie orientada S. Diremos que un punto $p \in S$ es un punto singular de v si $v(p) = 0$. El punto singular p es aislado si existe un entorno V de p en S tal que v no tiene más puntos singulares que p en V.

Nota.
A cada punto aislado p de un campo vectorial v en S se le puede asociar un entero. Sea $x : U \to S$ una parametrización ortogonal en el punto $p = x(0, 0)$ compatible con la orientación de S, y sea $\alpha : [0, l] \to S$ una curva parametrizada simple, cerrada y diferenciable a trozos tal que $\alpha([0, l]) \subset x(U)$ es el borde de una región simple que tiene a p como su único punto singular.

Definición 3.3.4. Se denomina índice de v en p al número $Ind(v, p)$ que representa el número de giros orientados que realiza el campo de vectores v al restringirse a la curva α si se considera esta con orientación positiva.

Nota.
Sea $v = v(t)$, $t \in [0, l]$ la restricción de v sobre α, y sea $\varphi = \varphi(t)$ una determinación diferenciable del ángulo orientado de x_u a $v(t)$. Entonces,

$$2\pi Ind(v, p) = \varphi(l) - \varphi(0) = \int_0^l \frac{d\varphi}{dt} dt$$

Proposición 3.3.1. *El* $Ind(v, p)$ *no depende ni de la parametrización* x*, ni de la curva* α *elegidas.*

Demostración. Por la interpretación de K en términos del transporte paralelo que se puede encontrar en el cap. 4.5 del *M. do Carmo*, *Differential Geometry of Curves and Surfaces*, el ángulo de rotación resultante ϕ depende de la curvatura integral de la siguiente forma

$$\Delta\phi = \phi(l) - \phi(0) = \iint_R K dA$$

Restando la ecuación anterior con la ecuación de la definición de índice tenemos

$$\iint_R K dA - 2\pi Ind(v, p) = (\phi - \varphi)(l) - (\phi - \varphi)(0) = \Delta(\phi - \varphi)$$

Como $\phi - \varphi$ no depende de x_u, el índice es independiente de la parametrización así como de la curva α.

□

Tomaremos ahora $S \subset \mathbb{R}^3$, una superficie orientada y compacta, y v un campo de vectores diferenciable con solo puntos singulares aislados. Se supondrá además que hay un número finito de ellos al que denotaremos n. Sea $\{x_\lambda\}$ una familia de parametrizaciones ortogonales compatibles con la orientación de S. Se considera una triangulación T de S tal que:

1. Todo triángulo $t \in T$ está contenido en algún entorno coordenado de la familia $\{x_\lambda\}$.
2. Todo $t \in T$ contiene a lo sumo un punto singular.
3. El borde de cada $t \in T$ no contiene puntos singulares y está orientado de forma positiva.

Si aplicamos la versión local del Teorema de Gauss-Bonnet a cada triangulo $t \in T$, sumamos los resultados y se tiene en cuenta que el borde de cada $t \in T$ aparece dos veces con orientaciones opuestas, entonces se obtiene

$$\iint_S K dA - 2\pi \sum_{i=1}^{n} Ind(v, p_i) = 0$$

Y, junto con el Teorema de Gauss Bonnet para superficies compactas, se tiene

$$\sum_{i=1}^{n} Ind(v, p_i) = \frac{1}{2\pi} \iint_S K dA = \chi(S)$$

De esta igualdad se obtiene el llamado “Teorema de Poincaré”:

Teorema 3.3.1 (Teorema de Poincaré). *La suma de los índices de un campo de vectores diferenciable v con puntos singulares aislados en una superficie compacta S es igual a la característica de Euler-Poincaré de S.*

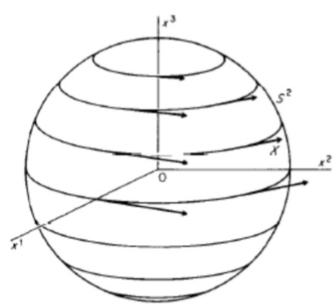
Nota.
El Teorema de Poincaré implica que la suma de los índices no depende de v, si no que solamente depende de la topología de la superficie S. En el caso de una superficie homeomorfa a la esfera $\mathbb{S}^2$, la suma de los índices de todo campo de vectores que tenga singularidades aisladas debe ser igual a $\chi(\mathbb{S}^2) = 2$. En particular, $\mathbb{S}^2$ no puede tener un campo de vectores diferenciables sin puntos singulares.
Si se considera la parametrización de la esfera de radio r y centro en el origen

$$x(\theta, \varphi) = (rsin(\theta)cos(\varphi), rsin(\theta)sin(\varphi), rcos(\theta))$$

para $0 < \theta < \pi$ y $0 < \varphi < 2\pi$, se obtiene el campo de vectores

$$x_\varphi(\theta, \varphi) = rsin(\theta)(-sin(\varphi) + cos(\varphi))$$

que puede ser extendido a un campo de vectores sobre la esfera de radio $r > 0$ con dos singularidades de índice 1 que se obtienen para $\theta = 0$ y $\theta = \pi$ es decir, en los polos de coordenadas $(0, 0, r)$ y $(0, 0, -r)$.



El Teorema de Poincaré es conocido popularmente como “Teorema de la Bola Peluda” y nos dice que siempre que queramos peinar una bola de forma que alisamos los pelos sobre la superficie de esta sin que el peinado tenga raya o ninguno de los pelos cambie bruscamente de dirección, siempre habrá algún remolino o algún pelo “tieso”.

Capítulo 4

Un curioso ejemplo.

Sean $\mathcal{B}$ y $\mathcal{C}$ dos anillos conmutativos, y sea t una indeterminada. En este capítulo se plantea la siguiente cuestión:

$$\text{Si } \mathcal{B}[t] \cong \mathcal{C}[t], \text{ ¿esto implica que } \mathcal{B} \cong \mathcal{C}?.$$

El objetivo de este capítulo será encontrar un contraejemplo que muestre que la implicación no se tiene porqué dar.

4.1. El isomorfismo en polinomios.

Sea $\mathbb{R}$ el cuerpo de los números reales y supongamos P, Q, t, U, V, W, X, Y, Z variables indeterminadas. Se construye el anillo de polinomios en tres variables con coeficientes reales $\mathbb{R}[X, Y, Z]$ que es también un $\mathbb{R}$-módulo.

Definición 4.1.1. A partir de ahora, se define el anillo $\mathcal{A}$ como el anillo cociente

$$\mathcal{A} = \mathbb{R}[X, Y, Z]/(X^2 + Y^2 + Z^2 - 1) = \mathbb{R}[x, y, z]$$

donde se entiende

$$x = X + (X^2 + Y^2 + Z^2 - 1)$$
$$y = Y + (X^2 + Y^2 + Z^2 - 1)$$
$$z = Z + (X^2 + Y^2 + Z^2 - 1)$$

al tomar las clases de equivalencia y por tanto, $x^2 + y^2 + z^2 = 1$.

Definición 4.1.2. Construimos el módulo libre $\mathcal{A}^3 = \mathcal{A} \oplus \mathcal{A} \oplus \mathcal{A}$ que es de rango 3 y se define la aplicación $\Phi : \mathcal{A}^3 \to \mathcal{A}$ definida por $\Phi(a, b, c) = ax + by + zc$ para $(a, b, c) \in \mathcal{A}^3$. Esta aplicación es un homomorfismo de $\mathcal{A}$-módulos.

Lema 4.1.1. *La sucesión* $0 \to Ker(\Phi) \hookrightarrow \mathcal{A}^3 \xrightarrow{\Phi} \mathcal{A} \to 0$ *es escindida.*

Demostración. El homomorfismo Φ es sobreyectivo ya que, como se tiene la relación $x^2 + y^2 + z^2 = 1$, todo elemento $a \in \mathcal{A}$ es imagen del elemento $(ax, ay, az) \in \mathcal{A}^3$ ($\Phi(ax, ay, az) = ax^2 + ay^2 + az^2 = a$). Por tanto, Φ induce la siguiente sucesión exacta:

$$0 \to Ker(\Phi) \hookrightarrow \mathcal{A}^3 \xrightarrow{\Phi} \mathcal{A} \to 0$$

Necesitamos definir un $\mathcal{A}$-homomorfismo $t : \mathcal{A} \to \mathcal{A}^3$ tal que $\Phi \circ t = 1_{\mathcal{A}}$. Sea $a \in \mathcal{A}$, mandaremos $a \mapsto (ax, ay, az) = a(x, y, z)$. Ahora,

$$\Phi \circ t(a) = \Phi(ax, ay, az) = ax^2 + ay^2 + az^2 = a(x^2 + y^2 + z^2) = a$$

y se tiene $\Phi \circ t = 1_{\mathcal{A}}$. Por tanto, la sucesión $0 \to Ker(\Phi) \to \mathcal{A}^3 \xrightarrow{\Phi} \mathcal{A} \to 0$ es exacta y escindida.

$\square$

Definición 4.1.3. Denotamos por $\mathbb{E}$ al núcleo del homomorfismo Φ, es decir, $\mathbb{E} = Ker(\Phi)$.

Nota.
Con esta notación, por el Lema de Escisión 1.4.2 se puede escibir $\mathcal{A}^3$ como la suma directa

$$\mathcal{A}^3 \cong \mathbb{E} \oplus \mathcal{A}$$

Definición 4.1.4. Para nuestro contraejemplo definiremos los $\mathcal{A}$-módulos $\mathcal{B} = \mathcal{A}[P, Q]$ y $\mathcal{C} = \mathcal{A}[U, V, W]/(xU + yV + zW)$.

Teorema 4.1.1. *Los* $\mathcal{A}$*-módulos* $\mathcal{B}[t]$ *y* $\mathcal{C}[t]$ *son isomorfos.*

Demostración. Consideramos el paso al álgebra simétrica $S(\mathcal{A}^3)$, y obtendremos los siguientes isomorfismos:

1. Por el Corolario 2.2.1, el álgebra simétrica del $\mathcal{A}$-módulo libre $\mathcal{A}^3$ de rango 3 es el álgebra de polinomios sobre $\mathcal{A}$ en tres variables, luego

$$S(\mathcal{A}^3) \cong \mathcal{A}[P, Q, t]$$

2. Por el isomorfismo de la Proposición 2.2.5 se tiene

$$S(\mathcal{A}^3) \cong S(\mathbb{E} \oplus \mathcal{A}) \cong S(\mathbb{E}) \otimes S(\mathcal{A})$$

3. De nuevo, por el resultado del Corolario 2.2.1 se cumple que $S(\mathcal{A}) \cong \mathcal{A}[t]$ y entonces

$$S(\mathbb{E}) \otimes S(\mathcal{A}) \cong S(\mathbb{E}) \otimes \mathcal{A}[t]$$

4. Por último, por el Corolario 1.7.1, se muestra que

$$S(\mathbb{E}) \oplus \mathcal{A}[t] \cong S(\mathbb{E})[t]$$

Es decir, tenemos la siguiente cadena de isomorfismos:

$$\mathcal{A}[P,Q,t] \cong S(\mathcal{A}^3) \cong S(\mathbb{E}) \otimes S(\mathcal{A}) \cong S(\mathbb{E}) \otimes \mathcal{A}[t] \cong S(\mathbb{E})[t]$$

Además, por la escisión de Φ se cumple también que

$$\mathcal{A}^3 \cong Ker(\Phi) \oplus t(\mathcal{A}) = Ker(\Phi) \oplus (x,y,z)\mathcal{A}$$

y por ser $Ker(\Phi)$ un submódulo de $\mathcal{A}^3$, al considerar la sucesión

$$0 \to \mathcal{A} \xrightarrow{t} \mathcal{A}^3 \xrightarrow{\pi} \mathcal{A}^3/t(\mathcal{A}) \to 0$$

donde π es la aplicación de paso al cociente, la sucesión es exacta y, además, es escindida porque si tomamos $\phi \in Hom_{\mathcal{A}}(\mathcal{A}^3, \mathcal{A})$ se tiene $\Phi \circ t = 1_{\mathcal{A}}$. Por el segundo teorema de isomorfía, que recordemos dice $L/(L \cap N) \cong (L+N)/N$, aplicado a $L = \mathbb{E}$ y $N = t(\mathcal{A})$ ($\mathbb{E} \cap t(\mathcal{A}) = 0$) se tiene que $\mathbb{E} \cong \mathcal{A}^3/(x,y,z)\mathcal{A}$. Ahora, tomando la base $\{(1,0,0),(0,1,0),(0,0,1)\}$ de $\mathcal{A}^3$, por el Corolario 2.2.1, se tiene el siguiente isomorfismo

$$S(\mathcal{A}^3) \xrightarrow{\sim} \mathcal{A}[U,V,W]$$

$$(1,0,0) \mapsto U$$

$$(0,1,0) \mapsto V$$

$$(0,0,1) \mapsto W$$

con $(x,y,z) = x(1,0,0) + y(0,1,0) + z(0,0,1)$, y el $S(\mathcal{A}^3)$-submódulo generado por $\mathcal{A}(x,y,z) \subset S(\mathcal{A}^3)$ será

$$\langle \mathcal{A}(x,y,z) \rangle = \langle (x,y,z) \rangle = (x,y,z) \cdot S(\mathcal{A}^3) = (xU + yV + zW)$$

Por la proposición 2.2.4, se tiene el isomorfismo

$$S(\mathbb{E}) \cong \mathcal{A}[U,V,W]/(xU + yV + zW) = \mathcal{C}$$

La anterior cadena de isomorfismos muestra que

$$\mathcal{B}[t] = \mathcal{A}[P,Q,t] \cong S(\mathbb{E})[t] = \mathcal{C}[t]$$

□

Definición 4.1.5. Denotaremos por ρ al isomorfismo de $\mathcal{A}$-álgebras $\mathcal{B}[t] \to \mathcal{C}[t]$. Este isomorfismo respeta $\mathcal{A}$, es decir, deja los elementos del anillo $\mathcal{A}$ fijos.

4.2. Generadores de $\mathbb{E}$.

Estudiaremos algunas propiedades de $\mathbb{E}$.

Definición 4.2.1. Dado $\alpha \in \mathcal{A}$ tal que $\alpha = P(X,Y,Z)+(X^2+Y^2+Z^2-1)$, su función polinómica asociada es $F_\alpha : \mathbb{S}^2 \to \mathbb{R}$ con $F_\alpha(a_1,a_2,a_3) = P(a_1,a_2,a_3)$.

Nota.
Sea $\alpha = P(X,Y,Z)+(X^2+Y^2+Z^2-1)$, la función polinómica F_α está bien definida ya que no depende de la elección del polinomio P. Si tomamos otro polinomio Q tal que $\alpha = Q(X,Y,Z)+(X^2+Y^2+Z^2-1)$, entonces

$$P(X,Y,Z)+(X^2+Y^2+Z^2-1) = Q(X,Y,Z)+(X^2+Y^2+Z^2-1) \Rightarrow$$

$$\Rightarrow P(X,Y,Z)-Q(X,Y,Z) = H(X,Y,Z)(X^2+Y^2+Z^2-1)$$

y para todo $(a_1,a_2,a_3) \in \mathbb{S}^2$,

$$F_\alpha(a_1,a_2,a_3) = P(a_1,a_2,a_3) \qquad F_\alpha(a_1,a_2,a_3) = Q(a_1,a_2,a_3)$$

pero, como por ser un punto de $\mathbb{S}^2$ cumple que $a_1^2+a_2^2+a_3^2 = 1$,

$$P(a_1,a_2,a_3)-Q(a_1,a_2,a_3) = H(a_1,a_2,a_3)(a_1^2+a_2^2+a_3^2-1) = 0$$

Definición 4.2.2. Se define un campo de vectores polinomial tangente a la esfera como una aplicación $\mathbb{X} : \mathbb{S}^2 \to \mathbb{R}^3$ tal que

1. Existen tres polinomios $P_1, P_2, P_3 \in \mathcal{A}$ tales que, para todo $p \in \mathbb{S}^2$,

$$\mathbb{X}(p) = (F_{P_1}(p), F_{P_2}(p), F_{P_3}(p))$$

2. $\mathbb{X}(p) \in T_p\mathbb{S}^2$, para todo $p \in \mathbb{S}^2$.

Nota.
Recordemos que dado un punto $p = (x,y,z) \in \mathbb{S}^2$, la condición de que un vector (A,B,C) en $\mathbb{R}^3$ pertenezca a $T_p\mathbb{S}^2$ significa que se cumple

$$(x,y,z)\cdot(A,B,C) = xA+yB+zC = 0$$

Proposición 4.2.1. *Cada elemento de $\mathbb{E}$ define un campo de vectores polinomial tangente a la esfera.*

Demostración. Sea $h \in \mathbb{E} = Ker(\Phi) = \mathcal{A}^3/(x,y,z)\mathcal{A}$. Entonces h es de la forma $h = (a,b,c)$ con $ax+by+cz = 0$. Ahora, h induce una aplicación de la esfera en $\mathbb{R}^3$:

$$\mathbb{X}_h : \mathbb{S}^2 \to \mathbb{R}^3$$

$$(a_1,a_2,a_3) \mapsto (F_a(a_1,a_2,a_3), F_b(a_1,a_2,a_3), F_c(a_1,a_2,a_3))$$

denotando por F_a, F_b y F_c las funciones polinómicas asociadas a los elementos a, b y c respectivamente. Si la función polinómica asociada a $ax+by+cz$ es

$F_{ax+by+cz} = xF_a + yF_b + zF_c$, como $ax + by + cz = 0$, esta función es la idénticamente nula: $F_{ax+by+cz} \equiv 0$. Entonces,

$$a_1 F_a(a_1, a_2, a_3) + a_2 F_b(a_1, a_2, a_3) + a_3 F_c(a_1, a_2, a_3) = F_{ax+by+cz}(a_1, a_2, a_3) = 0$$

Lo que significa que h define un campo de vectores polinomial tangente a la esfera porque para cada punto $p = (a_1, a_2, a_3) \in \mathbb{S}^2$, se tiene

$$(a_1, a_2, a_3) \cdot (F_a(p), F_b(p), F_c(p)) = F_{ax+by+cz}(a_1, a_2, a_3) = 0$$

y por tanto, $\mathbb{X}_h(p) = (F_a(p), F_b(p), F_c(p)) \in T_p\mathbb{S}^2$.

$\square$

Vamos a ver que se puede construir un campo de vectores en $\mathbb{S}^2$ dado un vector tangente cualquiera:

Lema 4.2.1. *Fijado un punto $p = (a_1, a_2, a_3) \in \mathbb{S}^2$, para todo vector v en el plano tangente $v = (v_1, v_2, v_3) \in T_p\mathbb{S}^2$, existe un campo de vectores polinomial tangente a la esfera $\mathbb{X} : \mathbb{S}^2 \to \mathbb{R}^3$ tal que $\mathbb{X}(p) = v$.*

Demostración. Podemos suponer a_3 distinto de 0 ya que una de las tres componentes del punto p debe ser no nula porque el punto $(0, 0, 0)$ no está en $\mathbb{S}^2$. Entonces, solo debemos tomar $P_1 = z\dfrac{v_1}{a_3}$ y $P_2 = z\dfrac{v_2}{a_3}$. Ahora, como el vector es tangente , despejamos v_3 de la igualdad $a_1v_1 + a_2v_2 + a_3v_3 = 0$ y se tiene $v_3 = -\dfrac{v_1a_1}{a_3} - \dfrac{v_2a_2}{a_3}$. De aquí, el polinomio P_3 debe ser $P_3 = -x\dfrac{v_1}{a_3} - y\dfrac{v_2}{a_3}$ y

$$xP_1 + yP_2 + zP_3 = x(z\frac{v_1}{a_3}) + y(z\frac{v_2}{a_3}) + z(-x\frac{v_1}{a_3} - y\frac{v_2}{a_3}) = 0$$

$\square$

Proposición 4.2.2. *$\mathbb{E}$ es un $\mathcal{A}$-módulo que no puede tener dos generadores.*

Demostración. Supongamos que $\mathbb{E}$ tiene dos generadores y llegaremos a una contradicción. Si $\mathbb{E}$ tuviera dos generadores $\{b_1, b_2\}$, para todo $h \in \mathbb{E}$ se podría escribir $h = \alpha b_1 + \beta b_2$ con $\alpha, \beta \in \mathcal{A}$. Sea $p_0 = (a_1, a_2, a_3)$ el punto en el que el campo de vectores tangete asociado a b_1 se anula, $\mathbb{X}_{b_1}(a_1, a_2, a_3) = (0, 0, 0)$, que sabemos que existe por el Teorema 3.3.1. Ahora, elegiremos un vector al que denotaremos $v_0 = (v_1, v_2, v_3) \in T_{p_0}\mathbb{S}^2$ tal que $v_0 \notin \langle \mathbb{X}_{b_2}(p_0) \rangle$. Por el Lema 4.2.1 existe un elemento $h_0 \in \mathbb{E}$ cumpliendo $\mathbb{X}_{h_0}(p_0) = v_0$. De esta forma, tomando los elementos $\alpha_0, \beta_0 \in \mathcal{A}$ tales que $h_0 = \alpha_0 b_1 + \beta_0 b_2$ se tendrá

$$v_0 = \mathbb{X}_{h_0}(p_0) = F_\alpha(p_0)\mathbb{X}_{b_1}(p_0) + F_\beta(p_0)\mathbb{X}_{b_2}(p_0) = F_\beta(p_0)\mathbb{X}_{b_2}(p_0)$$

pero el vector v_0 no está generado por b_2, luego tenemos una contradicción. Por tanto, $\mathbb{E}$ requiere al menos 3 generadores.

$\square$

4.3. Isomorfismo de $\mathcal{A}$-álgebras.

Probaremos ahora que $\mathcal{B}$ y $\mathcal{C}$ no son isomorfos. Para ello supondremos que existe un isomorfismo $\eta : \mathcal{B} \xrightarrow{\sim} \mathcal{C}$. El objetivo de este apartado es ver que si existe η, entonces tiene que ser un morfismo de $\mathcal{A}$-álgebras.

Lema 4.3.1. *Tanto $\mathcal{B}$ como $\mathcal{C}$ son $\mathcal{A}$-subálgebras del anillo de polinomios sobre $\mathcal{A}$ $\mathcal{B}[t] = \mathcal{A}[P, Q, t]$.*

Demostración. El hecho de que $\mathcal{B}$ es $\mathcal{A}$-subálgebra de $\mathcal{B}[t]$ es claro. Junto con el isomorfismo $\rho : \mathcal{C}[t] \to \mathcal{B}[t]$ (que es inyectivo), su restricción a $\mathcal{C}$ sigue siendo inyectiva y entonces $\mathcal{C}$ es una $\mathcal{A}$-subálgebra de $\mathcal{B}[t]$.

□

Veremos un resultado que utilizaremos más adelante.

Proposición 4.3.1. *Sea D un dominio y $P(t) \in D[t]$, $P(t) \neq 0$ con grado de $P(t)$ igual a n. Entonces no pueden existir $\alpha_1, \alpha_2, \ldots, \alpha_m \in D$ con $m > n$ tales que $P(\alpha_i) = 0$.*

Demostración. Si $\alpha \in D$ es una raíz del polinomio $P(t)$ con multiplicidad l, entonces $(t - \alpha)$ divide a $P(t)$ y se escribirá $P(t) = (t - \alpha)^l P_{n-l}(t)$ donde el grado de P_{n-l} es $n-l$. Ahora, si existieran raíces $\alpha_1, \alpha_2, \ldots, \alpha_m \in D$ con $m > n$ entonces se escribiría

$$P(t) = (t - \alpha_1) \ldots (t - \alpha_m)$$

pero grado$(P) = n$ y el grado de la parte derecha de la igualdad es m y se tenía $m > n$. Luego el polinomio $P(t)$ no puede tener un número de raíces (contando su multiplicidad) mayor que su grado n a menos que sea el polinomio nulo, $P(t) = 0 \in \mathbb{R}$.

□

Proposición 4.3.2. *Los únicos elementos invertibles de $\mathcal{A}$ son los números reales no nulos.*

Demostración. Supongamos α una unidad en $\mathcal{A}$. Entonces, α es de la forma

$$\alpha = P(X, Y, Z) + (X^2 + Y^2 + Z^2) = P(x, y, z)$$

con $P(X, Y, Z) \in \mathbb{R}[X, Y, Z]$. Recordemos que x, y y z son las clases en $\mathcal{A}$ de los elementos X, Y y Z respectivamente cumpliendo $x^2 + y^2 + z^2 = 1$. De aquí se tiene $x^2 = -y^2 - z^2 + 1$ y puedo elegir un polinomio $Q(X, Y, Z) \in \mathbb{R}[X, Y, Z]$ de la forma:

$$Q(X, Y, Z) = Q_0(Y, Z) + XQ_1(Y, Z)$$

con $Q_0(Y, Z), Q_1(Y, Z) \in \mathbb{R}[Y, Z]$ tal que $Q(x, y, z) = \alpha$, es decir, $Q(X, Y, Z)$ está en la misma clase que $P(X, Y, Z)$. Consideramos ahora otro polinomio

$T(X,Y,Z) \in \mathbb{R}[X,Y,Z]$ tal que $T(x,y,z)$ es el inverso de $Q(x,y,z)$, y elegimos el representante de la forma:

$$T(X,Y,Z) = T_0(Y,Z) + XT_1(Y,Z)$$

con $T_0(Y,Z), T_1(Y,Z) \in \mathbb{R}[Y,Z]$. De esta manera,

$$Q(X,Y,Z)T(X,Y,Z) = (Q_0(Y,Z) + XQ_1(Y,Z))(T_0(Y,Z) + XT_1(Y,Z)) =$$

$$= Q_0(Y,Z)T_0(Y,Z) + Q_0(Y,Z)XT_1(Y,Z) + XQ_1(Y,Z)T_0(Y,Z) + Q_1(Y,Z)X^2T_1(Y,Z) =$$
$$= 1 + H(X,Y,Z)(X^2 + Y^2 + Z^2 - 1)$$

Podemos ver que el polinomio $H(X,Y,Z)$ es un polinomio en las variables Y, Z ya que si tuviera variable X, al multiplicarlo por $(X^2 + Y^2 + Z^2 - 1)$, esta aparecería al menos elevada al cubo, mientras que al multiplicar $Q(X,Y,Z)$ por $T(X,Y,Z)$ el término de mayor grado en X es de grado dos. Entonces, $H(X,Y,Z) = H(Y,Z) \in \mathbb{R}[Y,Z]$. Ahora, igualando en ambos lados los coeficientes de X^0, X^1, y X^2 se tiene que

$$Q_0(Y,Z)T_0(Y,Z) = 1 + H(Y,Z)(Y^2 + Z^2 - 1)$$

$$Q_0(Y,Z)T_1(Y,Z) + Q_1(Y,Z)T_0(Y,Z) = 0$$
$$Q_1(Y,Z)T_1(Y,Z) = H(Y,Z)$$

Sea $D(Y,Z) = \text{m.c.d}(T_0(Y,Z), T_1(Y,Z))$. Escribimos

$$T_0(Y,Z) = D(Y,Z)B_0(Y,Z)$$

$$T_1(Y,Z) = D(Y,Z)B_1(Y,Z)$$

de forma que $B_0(Y,Z)$ y $B_1(Y,Z)$ no tienen factores comunes (lo que quiere decir que $\text{m.c.d}(B_0(Y,Z), B_1(Y,Z)) = 1$). De la ecuación correspondiente a los coeficientes de X^1 se obtiene que

$$Q_1(Y,Z)D(Y,Z)B_0(Y,Z) = -Q_0(Y,Z)D(Y,Z)B_1(Y,Z)$$

y de aquí

$$Q_1(Y,Z)B_0(Y,Z) = -Q_0(Y,Z)B_1(Y,Z)$$

Como $B_0(Y,Z)$ no divide a $B_1(Y,Z)$ entonces tiene que dividir a $Q_0(Y,Z)$ y se tiene

$$Q_0(Y,Z) = T(Y,Z)B_0(Y,Z)$$

y, de igual forma, $B_1(Y,Z)$ debe dividir a $Q_1(Y,Z)$, y se tiene

$$Q_1(Y,Z) = -T(Y,Z)B_1(Y,Z)$$

Por tanto, sustituyendo en la ecuación correspondiente a los coeficientes de X^2:

$$H(Y,Z) = Q_1(Y,Z)T_1(Y,Z) = -D(Y,Z)T(Y,Z)B_1^2(Y,Z)$$

Ahora, por la ecuación correspondiente a los coeficientes de grado 0,

$$Q_0(Y,Z)T_0(Y,Z) = D(Y,Z)T(Y,Z)B_0^2(Y,Z) =$$

$$= 1 + H(Y,Z)(Y^2+Z^2-1) = 1 - D(Y,Z)T(Y,Z)B_1^2(Y,Z)(Y^2+Z^2-1)$$

de donde se deduce que $D(Y,Z)$ y $T(Y,Z)$ dividen a 1, luego $D(Y,Z)$, $T(Y,Z)$ están en $\mathbb{R}$. De ahora en adelante los denotaremos $D(Y,Z) = d$ y $T(Y,Z) = t$ y, entonces tendremos

$$T_0(Y,Z) = dB_0(Y,Z)$$

$$T_1(Y,Z) = dB_1(Y,Z)$$

y además

$$dtB_0^2(Y,Z) = 1 - dtB_1^2(Y,Z)(Y^2+Z^2-1)$$

Si se prueba que $B_1(Y,Z) = 0$ entonces $T_1(Y,Z)$ también será igual a 0 y, además, $dtB_0^2(Y,Z) = 1$ de donde se deduce que $B_0(Y,Z) \in \mathbb{R}$. De aquí se tendrá $T_0(Y,Z) \in \mathbb{R}$. Escribimos la última igualdad como

$$1 = dt(B_0^2(Y,Z) + B_1^2(Y,Z)(Y^2+Z^2-1))$$

Veamos que hay infinitas $\alpha \in \mathbb{R}[Y]$ tales que para $B_1[Y,Z] \in \mathbb{R}[Y][Z]$ se tiene $B_1[Y,\alpha] = 0 \in \mathbb{R}[Y]$. Retomando la última ecuación y sustituyendo la variable Z por $\alpha \in \mathbb{R}$ se tiene:

$$1 = dt(B_0^2(Y,\alpha) + B_1^2(Y,\alpha)(Y^2+\alpha^2-1))$$

Lo que nos quedan son polinomios en una variable Y en el lado derecho y la constante 1 en el lado izquierdo. Como los polinomios B_0 y B_1 aparecen elevados al cuadrado y además el polinomio B_1 está multiplicando a Y^2, la única forma de que se cumpla la igualdad es que los términos de mayor grado de los dos sumandos del lado derecho de la ecuación se anulen entre sí, ya que en el lado izquierdo la variable Y no aparece. Para que se puedan anular, ambos sumandos deben tener el mismo grado, es decir, si el grado de B_1 es n, al multiplicarlo por Y^2 el grado del sumando $B_1^2(Y,\alpha)(Y^2+\alpha^2-1)$ será $2n+2$. De esto deducimos que el grado de B_0 debe ser $n+1$ para que al elevarlo al cuadrado nos quede grado $2n+2$. Si denotamos

$$B_0(Y,\alpha) = \sum_{i=0}^{n+1} \gamma_i Y^i$$

$$B_1(Y,\alpha) = \sum_{j=0}^{n} \delta_j Y^j$$

al igualar el coeficiente de Y^{2n+2}, tendremos

$$0 = \gamma_{n+1}^2 + \delta_n^2$$

pero hemos supuesto que, al menos $\delta_n \neq 0$, por lo que $\delta_n^2 > 0$ y la igualdad no se puede dar. Luego $B_1(Y, \alpha) = 0$ y esto ocurre para todas las $\alpha \in \mathbb{R}$ y por la Proposición 4.3.1, $B_1(Y, Z) = 0$.
Por lo visto anteriormente,

$$B_1(Y,Z) = 0 \Rightarrow T_1(Y,Z) = 0 \Rightarrow T(X,Y,Z) = T_0(Y,Z) \Rightarrow$$
$$\Rightarrow \alpha^{-1} = T_0(Y,Z) + (X^2 + Y^2 + Z^2 - 1)$$
$$B_1(Y,Z) = 0 \Rightarrow Q_1(Y,Z) = 0 \Rightarrow Q(X,Y,Z) = Q_0(Y,Z) \Rightarrow$$
$$\Rightarrow \alpha = Q_0(Y,Z) + (X^2 + Y^2 + Z^2 - 1)$$

y, por otra parte

$$B_0(Y,Z) \in \mathbb{R} \Rightarrow T_0(Y,Z), Q_0(Y,Z) \in \mathbb{R}$$

En conclusión, α y su inverso α^{-1} son reales no nulos.

□

Lema 4.3.2. *Si existe el isomorfismo $\eta : \mathcal{B} \to \mathcal{C}$, entonces es un $\mathbb{R}$-isomorfismo ($\eta(\mathbb{R}) = \mathbb{R}$).*

Demostración. Los únicos elementos invertibles de $\mathcal{A}$ son los reales no nulos. Entonces, se tendrá que el conjunto de los elementos invertibles de $\mathcal{B}[t]$ es $\mathbb{R}^*$ por ser $\mathcal{B}[t] = \mathcal{A}[P,Q][t]$, y también los de $\mathcal{B}$. Además, por ser ρ un isomorfismo, las unidades de $\mathcal{C}[t]$ serán las imágenes por ρ de los números reales no nulos. En consecuencia, los únicos elementos invertibles de $\mathcal{C}$ es el conjunto $\mathbb{R}^*$. Entonces, como el isomorfismo η lleva unidades en unidades, se tiene que $\eta(\mathbb{R}) \subset \mathbb{R}$ y $\eta^{-1}(\mathbb{R}) \subset \mathbb{R}$. Por tanto, $\eta|_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}$. Pero se sabe que $\mathbb{R}$ no tiene automorfismos no triviales ($Aut\mathbb{R} = \{1_{\mathbb{R}}\}$), luego η debe ser un $\mathbb{R}$-isomorfismo .

□

Queremos ahora definir un pre-orden en $\mathcal{A}$. Para ello debemos recordar algunos resultados.

Definición 4.3.1. Se define una relación de pre-orden en un conjunto S como una relación binaria $\geq$ que cumple las propiedades reflexiva y transitiva.

Definición 4.3.2. Dado un anillo A y una relación de pre-orden $\geq$ en A, diremos que A es un anillo preordenado si para x, y, $z \in A$ se cumplen las siguientes propiedades:

1. Para x, y tales que $x \geq y \Rightarrow x + z \geq y + z$ para todo z.
2. Para $x \geq 0$ e $y \geq 0 \Rightarrow xy \geq 0$.

Definición 4.3.3. Si además se cumple la propiedad antisimétrica ($x \geq y$ e $y \geq x \Rightarrow x = y$ para $x, y \in A$), el anillo A será un anillo parcialmente ordenado.

Proposición 4.3.3. *El anillo $\mathcal{A}$ es un anillo preordenado.*

Demostración. Definiremos un pre-orden en base a las funciones polinómicas asociadas a los elementos de $\mathcal{A}$. Se tiene $\mathbb{R} \subset \mathcal{A}$, y si denotamor por $P(\mathbb{S}^2)$ al conjunto de las funciones polinómicas en $\mathbb{S}^2$, también $\mathbb{R} \subset P(\mathbb{S}^2)$: las funciones constantes. Podemos establecer una aplicación $\mathcal{A} \to P(\mathbb{S}^2)$ enviando a cada elemento $\alpha \in \mathcal{A}$ en su función polinómica asociada F_α. Siendo así, podemos definir en $\mathcal{A}$ una relación binaria como sigue: dados $\alpha, \beta \in \mathcal{A}$, diremos que $\alpha \geq \beta$ $\Leftrightarrow F_\alpha(a_1, a_2, a_3) \geq F_\beta(a_1, a_2, a_3)$, para todo $(a_1, a_2, a_3) \in \mathbb{S}^2$. Es claro que esta relación cumple las propiedades reflexiva y transitiva, luego hemos definido un pre-orden.
Veamos ahora que este pre-orden convierte al anillo $\mathcal{A}$ en un anillo preordenado:

1. Para $\alpha, \beta \in \mathcal{A}$ tales que $\alpha \geq \beta$ se tiene $F_\alpha(a_1, a_2, a_3) \geq F_\beta(a_1, a_2, a_3)$, entonces:

$$F_{\alpha+\gamma}(a_1, a_2, a_3) = F_\alpha(a_1, a_2, a_3) + F_\gamma(a_1, a_2, a_3) \geq$$

$$\geq F_\beta(a_1, a_2, a_3) + F_\gamma(a_1, a_2, a_3) = F_{\beta+\gamma}(a_1, a_2, a_3)$$

   Luego $\alpha + \gamma \geq \beta + \gamma$ para todo $\gamma \in \mathcal{A}$.

2. Si $\alpha \geq 0$ y $\beta \geq 0 \Rightarrow F_\alpha(a_1, a_2, a_3) \geq 0$ y $F_\beta(a_1, a_2, a_3) \geq 0$, entonces

$$F_{\alpha\beta}(a_1, a_2, a_3) = F_\alpha(a_1, a_2, a_3) F_\beta(a_1, a_2, a_3) \geq 0$$

   Luego $\alpha\beta \geq 0$.

$\square$

Lema 4.3.3. *Si D es un anillo preordenado y tomamos dos polinomios P, Q en $D[t]$ tales que $P = \sum \alpha_i t^i$ con $n = grado(P)$ y $Q = \sum \beta_j t^j$ con $s = grado(Q)$. Entonces la relación dada por $P \geq Q \Leftrightarrow$ ó $n > s$ ó bien $n = s$ y $\alpha_n \geq \beta_s$ convierte a $D[t]$ en un anillo preordenado.*

Demostración. En primer lugar, la relación del enunciado es un pre-orden: sean $P, Q \in D[t]$ como en el enunciado, y $R = \sum \gamma_k t^k$ con $r = grado(R)$:

1. Para P se cumple $P \geq P$ ya que $n = n$ y $\alpha_n \geq \alpha_n$ por ser D preordenado.
2. Para P, Q, R cumpliendo $P \geq Q$ y $Q \geq R$ se tienen las siguientes posibilidades:
   - Si $n > s$ y $s > r \Rightarrow n > r$ y entonces $P \geq R$.
   - Si $n > s$ y $s = r \Rightarrow n > r$ y entonces $P \geq R$.
   - Si $n = s$ y $s > r \Rightarrow n > r$ y entonces $P \geq R$.
   - Si $n = s$ con $\alpha_n \geq \beta_s$ y $s = r$ con $\beta_s \geq \gamma_r \Rightarrow n = r$ con $\alpha_n \geq \gamma_r$ por ser D preordenado y entonces $P \geq R$.

Entonces, falta ver que $D[t]$ cumple las propiedades de anillo preordenado:

1. Para P, Q tales que $P \geq Q$

   - $n > s \Rightarrow n + r > s + r$.
   - $n = s$ y $\alpha_n \geq \beta_s \Rightarrow \alpha_n + \gamma_r \geq \beta_s + \gamma_r$ por ser D preordenado.

   Luego $P + R \geq Q + R$ para todo Q.

2. Si $P \geq 0$ y $Q \geq 0 \Rightarrow \alpha_n \geq 0$ y $\beta_s \geq 0 \Rightarrow \alpha_n\beta_s \geq 0$ por ser D preordenado y entonces $PQ \geq 0$.

□

Lema 4.3.4. *Supongamos D un anillo preordenado y sean P, Q, R tres polinomios en $D[t]$ cumpliendo $P^2 + Q^2 + R^2 = 1$. Entonces P, Q, R son elementos de D.*

Demostración. Supongamos $P, Q, R \in D[t] \setminus D$ de la forma: $P = \sum \alpha_i t^i$ con $n = grado(P)$, $Q = \sum \beta_j t^j$ con $s = grado(Q)$ y $R = \sum \gamma_k t^k$ con $r = grado(R)$. Sea $m = \max\{n, s, r\}$ el máximo de los grados. Los polinomios P, Q y R cumplen la ecuación:

$$P^2 + Q^2 + R^2 = 1$$

Entonces, igualando los coeficientes de t^m en cada lado tendremos:

$$\alpha_m^2 + \beta_m^2 + \gamma_m^2 = 0$$

La suma de cuadrados siempre debe ser positiva o cero, pero al menos uno de los coeficientes α_m,β_m y γ_m es distinto de 0, luego tenemos una contradicción. Entonces, P, Q, R son elementos de D.

□

Lema 4.3.5. *Tanto $\mathcal{B}$ como $\mathcal{C}$ cumplen: Dados a, b, c en el $\mathcal{A}$-módulo cumpliendo $a^2 + b^2 + c^2 = 1$, entonces a, b, c están en el anillo $\mathcal{A}$.*

Demostración. Hemos definido un pre-orden en $\mathcal{A}$, y por el Lema 4.3.3 el anillo $\mathcal{A}[P]$ vuelve a ser un anillo preordenado. Por este mismo Lema, como $\mathcal{B}$ se define por $\mathcal{B} = \mathcal{A}[P, Q] = \mathcal{A}[P][Q]$ se tiene que $\mathcal{B}$ es también un anillo preordenado.
Por ser $\mathcal{B}$ preordenado, de la misma manera $\mathcal{B}[t]$ es un anillo preordenado. El hecho de que $\mathcal{C}$ sea preordenado se obtiene de que $\mathcal{C}[t]$ y $\mathcal{B}[t]$ son isomorfos mediante el isomorfismo ρ que respeta el anillo $\mathcal{A}$ y por tanto, podemos llevarlo a $\mathcal{C}[t]$, y finalmente restringirlo a $\mathcal{C}$, luego $\mathcal{C}$ es un anillo preordenado.
Ahora, aplicando el Lema 4.3.4 se concluye la demostración.

□

Proposición 4.3.4. *Si existe el isomorfismo de anillos η, entonces existe un isomorfismo η' tal que η' es un $\mathcal{A}$-isomorfismo.*

Demostración. Queremos ver que $\eta(\mathcal{A}) \subset \mathcal{A}$. Para ello, basta con comprobar que $\eta(x)$, $\eta(y)$ y $\eta(z) \in \mathcal{A}$ ya que η es un $\mathbb{R}$-isomorfismo y $\mathcal{A} = \mathbb{R}[x, y, z]$. Por ser $\eta : B \to C$ un $\mathbb{R}$-isomorfismo, $\eta(1) = 1$ y entonces:

$$\eta(x^2 + y^2 + z^2) = \eta(1) = 1$$

y, por otra parte,

$$\eta(x^2 + y^2 + z^2) = \eta(x^2) + h(y^2) + \eta(z^2) = \eta(x)^2 + \eta(y)^2 + \eta(z)^2 = \eta(1) = 1$$

Pero hemos visto que las únicas soluciones de esta ecuación en $\mathcal{B} = \mathcal{A}[P][Q]$ están en $\mathcal{A}[P]$ y, a su vez, las únicas soluciones de esta ecuación en $\mathcal{A}[P]$ están en $\mathcal{A}$ de donde se deduce que $\eta(x)$, $\eta(y)$ y $\eta(z) \in \mathcal{A}$. Por lo tanto, $\eta(\mathcal{A}) \subset \mathcal{A}$. De forma similar, $\eta^{-1}(\mathcal{A}) \subset \mathcal{A}$, ya que $\eta^{-1}(1) = 1$ y dados $a, b, c \in \mathcal{C}$ tales que $a^2 + b^2 + c^2 = 1$, entonces

$$\eta^{-1}(a^2 + b^2 + c^2) = \eta^{-1}(a)^2 + \eta^{-1}(b)^2 + \eta^{-1}(c)^2 = \eta -^{-1} (1) = 1$$

y $\eta^{-1}(a), \eta^{-1}(b), \eta^{-1}(c) \in \mathcal{B} \Rightarrow \eta^{-1}(a), \eta^{-1}(b), \eta^{-1}(c) \in \mathcal{A}$. Con esto hemos probado que $\eta(\mathcal{A}) \subset \mathcal{A}$.
Si ahora consideramos el $\mathcal{B}$-automorfismo φ que coincide con la restricción en $\mathcal{A}$ de la inversa de η, y deja fijos los elementos P y Q de $\mathcal{B} = \mathcal{A}[P, Q]$, es decir:

$$\begin{array}{rcl} \varphi : \mathcal{B} & \longrightarrow & \mathcal{B} \\ P & \longmapsto & P \\ Q & \longmapsto & Q \\ a & \longmapsto & \eta^{-1}|_{\mathcal{A}}(a), \quad a \in \mathcal{A} \end{array}$$

y tomamos su composición con η,a la que denotaremos por η', $\eta \circ \varphi : \mathcal{B} \to \mathcal{C}$ se tiene:

$$\begin{array}{rcl} \eta' : \mathcal{B} & \longrightarrow & \mathcal{C} \\ P & \longmapsto & \eta(P) \\ Q & \longmapsto & \eta(Q) \\ a & \longmapsto & \eta(\eta^{-1}|_{\mathcal{A}}(a)) = a, \quad a \in \mathcal{A} \end{array}$$

En consecuencia, $\eta'|_{\mathcal{A}} = 1_{\mathcal{A}}$ y se puede asumir que η' es un $\mathcal{A}$-isomorfismo de $\mathcal{B}$ y $\mathcal{C}$. De ahora en adelante, denotaremos a η' por η.

□

4.4. Conclusión.

Proposición 4.4.1. *Si existe el isomorfismo η, la componente de $\mathcal{C}$ de grado uno tiene dos generadores.*

Demostración. El hecho de que $\mathcal{C}$ sea una $\mathcal{A}$-álgebra graduada se obtiene de que el ideal $(xU + yV + zW)$ es homogéneo. Entonces tenemos un $\mathcal{A}$-isomorfismo entre dos álgebras graduadas $\mathcal{B} = \oplus B_n$ y $\mathcal{C} = \oplus C_s$ tales que $B_0 = \mathcal{A}$ y $C_0 = \mathcal{A}$. Por ser η un isomorfismo de $\mathcal{A}$-álgebras, sabemos que $\mathcal{C}$ estará generado por los elementos $\eta(P)$ y $\eta(Q)$. Si se denotan por $c = \eta(P)$ y $c' = \eta(Q)$, entonces $\mathcal{C} = \mathcal{A}[c, c']$ y teniendo en cuenta la descomposición homogénea de cada uno de ellos,

$$c = c_0 + c_1 + \dots c_n$$

$$c' = c'_0 + c'_1 + \dots c'_s$$

Ahora, se consideran los elementos $x = c - c_0$ y $x' = c' - c'_0$, y dado un elemento $\gamma \in \mathcal{C}$, se tiene

$$\gamma = \sum_{i,j} a_{i,j} c^i c'^j = \sum_{i,j} a_{i,j} (x + c_0)^i (x' + c'_0)^j =$$

$$= a_{10}x + a_{10}c_0 + a_{01}x' + a_{01}c'_0 + a_{11}xx' + a_{11}c'_0x + a_{11}c_0x' + a_{11}c_0c'_0 +$$
$$+ a_{21}x^2x' + 2a_{21}c_0xx' + a_{21}c_0^2x' + a_{21}c'_0x^2 + 2a_{21}c_0c'_0x + a_{21}c_0^2c'_0 +$$
$$+ a_{12}xx'^2 + 2a_{12}c'_0xx' + a_{12}c'^2_0x + a_{12}c_0x'^2 + 2a_{12}c_0c'_0x' + a_{12}c_0c'^2_0 + \dots$$

y si denotamos por b_{ij} a la suma de los coeficientes de los monomios de grado i en x y grado j en x', se puede escribir

$$\gamma = \sum_{i,j} b_{i,j} x^i x'^j$$

Entonces, podemos suponer el álgebra $\mathcal{C}$ generado por los elementos $x = c - c_0$ y $x' = c' - c'_0$ que no tienen componente homogénea de grado cero, es decir, $\mathcal{C} = \mathcal{A}[x, x']$. De modo que, para un elemento $\gamma \in \mathcal{C}$ tenemos, por un lado su descomposición homogénea $\gamma = \sum_{l \geq 0} \gamma_l$, y por otro,

$$\gamma = \sum_{i,j} b_{i,j} x^i x'^j = \sum_{i,j} b_{i,j} (c_1 + c_2 + \dots + c_n)^i (c'_1 + c'_2 + \dots + c'_s)^j$$

y comparando en ambas igualdades obtenemos que la componente homogénea de grado uno de γ se escribe como

$$\gamma_1 = b_{10}c_1 + b_{01}c'_1$$

de donde se deduce que la componente de $\mathcal{C}$ de grado uno C_1 está generada como $\mathcal{A}$-módulo por los elementos c_1 y c'_1.

$\square$

Por último, tenemos el resultado que dará respuesta a la pregunta planteada al principio del capítulo.

Teorema 4.4.1. *$\mathcal{B}$ y $\mathcal{C}$ no son isomorfos.*

Demostración. Recordemos que $\mathcal{C} = \mathcal{A}[U,V,W]/(xU + yV + zW)$. Entonces la componente de grado 1 será $C_1 = (\mathcal{A}[U,V,W])_1/(xU + yV + zW)_1$ por cómo se construye la graduación en un cociente. No obstante, los elementos de $(\mathcal{A}[U,V,W])_1$ son los polinomios de grado 1, dicho de otra manera, el conjunto $\{aU + bV + cW/a, b, c \in \mathcal{A}\}$ y este conjunto es isomorfo a $\mathcal{A}^3$. Por otro lado, $(xU + yV + zW)_1 = \{\alpha(xU + yV + zW)/\alpha \in \mathcal{A}\} = (x, y, z)\mathcal{A}$. En consecuencia,

$$C_1 = (\mathcal{A}[U,V,W])_1/(xU + yV + zW)_1 \cong \mathcal{A}^3/(x, y, z)\mathcal{A} \cong \mathbb{E}$$

de donde se obtiene una contradicción ya que $\mathbb{E} = Ker(\Phi)$ hemos visto no podía estar generado por dos generadores. De aquí se concluye que no existe el isomorfismo $\eta : \mathcal{B} \xrightarrow{\sim} \mathcal{C}$ que se había supuesto en un principio, y por tanto, $\mathcal{B}$ y $\mathcal{C}$ no son isomorfos.

$\square$

Bibliografía

[1] M.F.ATIYAH AND I.G. MACDONALD. *Introduction to Commutative Algebra.*
Addison-Wesley Publishing Company,1969.

[2] BOURBAKI, N. *Éléments de Mathématique. ÁLGEBRE. Chapitres 1 à 3.*
2ème ed. Réimpression inchangée de lédition originale de 1970. N.Bourbaki et Springer-Verlag, Berlin Heidelberg, 2007.

[3] SINGH, B. *Basic Commutative Algebra.*
World Scientific Punblishing Co. Pte. Ltd, 2011.

[4] HIDEYUKI MATSUMURA. *Commutative Algebra.*
The Benjamin/Cummings Publishin Company, 1980.

[5] MANFREDO P. DO CARMO. *Differential Geometry of curves and Surfaces.*

[6] JOSE ANGEL HERMIDA ALONSO, MARIA LUISA CARRILLO DE ALBORNOZ, JUAN GABRIEL TENA AYUSO. *Álgebra Local.*
Universidad de Valladolid. Secretariado de Publicaciones, 1985.

[7] S.LANG. *Algebra.*
Versión española de MILAGROS ANCOCHEA. Aguilar, 1977.

[8] LEONARD GILLMAN AND MEYER JERISON. *Rings of Continuous Functions.*
Springer-Verlag, 1960.