TEMA 1.

1. INTRODUCCIÓN

En este capítulo vamos a estudiar nociones básicas de teoría de anillos. Introduciremos las nociones de anillo, subanillo, anillo conmutativo, anillo unitario, anillo de división y cuerpo. Estudiaremos las aplicaciones naturales entre anillos: los homomorfismo de anillos. Veremos algunas propiedades fundamentales de la estructura de anillo e iremos introduciendo, tanto ejemplos: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ o $\mathbb{Z}_n$ (el anillo de congruencias módulo n), como construcciones de nuevos anillos a partir de otros conocidos: el anillo suma directa, el anillo producto cartesiano, el anillo de endomorfismos de un grupo abeliano o los anillos de matrices.

2. DEFINICIÓN BÁSICAS.

2.1 DEF. Un **anillo** es una terna $(R, +, .)$ en donde R es un conjunto y "+", "." son dos operaciones en R tales que:

(1). $(R, +)$ es un grupo abeliano:

- Propiedad asociativa: $(a + b) + c = a + (b + c)$ para todo $a, b, c \in R$.
- Elemento neutro: existe $0 \in R$ tal que $a + 0 = 0 + a$ para todo $a \in R$
- Elemento opuesto: para todo $a \in R$ existe $-a \in R$ tal que $a + (-a) = (-a) + a = 0$.
- Propiedad conmutativa: $a + b = b + a$ para todo $a, b \in R$.

(2). $(R, .)$ verifica la propiedad asociativa: $(a.b).c = a.(b.c)$ para todo $a, b, c \in R$.

(3). Se verifican las propiedades distributivas: para todos $a, b, c \in R$,

$$(a + b).c = a.c + b.c \qquad c.(a + b) = c.a + c.b$$

$\star$ Diremos que un **anillo** $(R, +, .)$ es **conmutativo** si "." es conmutativa.

$\star$ Diremos que un **anillo** $(R, +, .)$ es **unitario** si "." es una operación unitaria y R tiene más de un elemento.

Nota: La primera operación se llamará **suma**. El neutro de la suma lo denotaremos por 0. Al inverso de la suma lo llamaremos **opuesto**. La segunda

operación se llamará **producto** y la denotaremos por yuxtaposición. Al neutro del producto lo denotaremos, si existe, por 1. Al inverso del producto, si existe, se llamara **inverso**.

2.2 Ejemplos. (1). Si consideramos $(G,+)$ un grupo abeliano y definimos un producto en G por: $a.b := 0$ para todo $a, b \in G$, $(G,+,.)$ tiene estructura de anillo conmutativo.

(2). $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ con las operaciones usuales (todos son anillos conmutativos y unitarios). $\mathcal{M}_n(\mathbb{R})$, el anillo de matrices sobre los Reales, con las operaciones usuales (anillo unitario, no conmutativo para $n \geq 2$). $2\mathbb{Z}$ con las operaciones usuales de $\mathbb{Z}$ (anillo conmutativo no unitario).

(3). Los anillos realmente no tienen que ser de "números": sea X un conjunto no vacío y denotemos por $\mathcal{P}(X)$ el conjunto de partes de X. Entonces $(\mathcal{P}(X), \triangle, \cap)$ tiene estructura de anillo conmutativo y unitario.

Nota: $\triangle$ denota la diferencia simétrica: dados $A, B \subset X$,

$$A \triangle B := (A - B) \cup (B - A) = (A \cap B^c) \cup (B \cap A^c)$$

(4). Los anillos módulo n: Sea n un número natural y consideremos $\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$. Observar que $\mathbb{Z}_n$ tiene n elementos. Dados $a, b \in \mathbb{Z}_n$ definimos:

– La suma de a y b como el resto de dividir $a + b$ por n.

$\star$ $(\mathbb{Z}_n, +)$ es el grupo abeliano ya estudiado en el primer cuatrimestre.

– El producto de a y b como el resto de dividir $a.b$ por n.

Entonces $(\mathbb{Z}_n, +, \ )$ tiene estructura de anillo conmutativo y unitario.

2.3 Proposición. Sea $(R,+,.)$ un anillo. Entonces:

(1) $0.a = a.0 = 0$ para todo $a \in R$.

(2) $a.(-b) = (-a).b = -(a.b)$ para todo $a, b \in R$.

Si además R es unitario,

(3) la unidad es única.

(4) Si $a \in R$ es un elemento inversible, el inverso de a es único (al que denotaremos por a^{-1}).

2.4 Def. A los elementos inversibles de un anillo R se les denomina unidades. El conjunto de las unidades de un anillo R se denota por $\mathcal{U}(R)$.

Nota: $(\mathcal{U}(R), .)$ tiene estructura de grupo. Es más, si R es conmutativo, $\mathcal{U}(R)$ es un grupo abeliano.

2.5 Def. Se dice que un anillo $(R, +, .)$ es un **anillo de división** si es unitario y todo elemento no nulo de R tiene inverso. Si además es conmutativo, se dice que es un **cuerpo**.

Nota: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ son cuerpos.

Podríamos pensar que la propiedad que poseen $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, o $\mathbb{C}$: si $a.b = 0$, entonces $a = 0$ o $b = 0$ es cierta para todo anillo. Veamos un contraejemplo: en $\mathbb{Z}_{12}$, $\bar{6}.\bar{4} = \bar{0}$ y ni $\bar{6}$ ni $\bar{4}$ son nulos.

2.6 Def. Sea R un anillo. Se dice que un elemento no nulo $a \in R$ es un **divisor de cero por la izquierda** si existe un elemento no nulo $b \in R$ tal que $a.b = 0$. de manera análoga se define **divisor de cero por la derecha**. Un anillo conmutativo y unitario sin divisores de cero por la izquierda y por la derecha se denomina un **dominio de integridad**.

Nota: Todo cuerpo es un dominio de integridad. $\mathbb{Z}$ es un dominio de integridad que no es cuerpo.

2.7 Def. Sea $(R, +, .)$ un anillo. Se dice que $A \subset R$ es un subanillo de R, y se representa $A \leq R$, si:

- La suma de R es una operación interna en A: $a + b \in A$ para todos $a, b \in A$
- El producto de R es una operación interna en A: $ab \in A$ para todos $a, b \in A$
- $(A, +, .)$ tiene estructura de anillo.

Nota: Por tanto, para demostrar que un subconjunto A de un anillo R es un subanillo tenemos que demostrar 9 propiedades. No obstante algunas son triviales:

$\star$ Si demostramos que la suma y el producto son operaciones internas, el carácter asociativo y conmutativo de la suma, el carácter asociativo del producto y las propiedades distributivas son validas para todo R, por tanto son validas para elementos de A.

$\star$ hay que comprobar que $0 \in A$ y que A contiene todos sus opuestos.

Luego para demostrar que A es un subanillo de un anillo R sólo tenemos que demostrar que $(A, +)$ es subgrupo y que el producto es cerrado en A.

2.8 Ejemplo. $2\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

Nota: Un subanillo de un anillo unitario no tiene que ser unitario. Es más, aunque sea unitario la unidad del anillo y del subanillo no tiene que coincidir. (Por resultados del primer cuatrimestre, el neutro de la suma si que coincide)

Nota: Todo subanillo de un dominio de integridad es un dominio de integridad. En particular, todo subanillo de un cuerpo es un dominio de integridad.

3. HOMOMORFISMOS DE ANILLOS

3.1 Def. Sean $(R, +, .)$ y $(R', +', .')$ dos anillos. Se define un **homomorfismo** de R en R' como una aplicación $f : R \to R'$ tal que:

$$f(a+b) = f(a) +' f(b) \quad \text{para todo } a, b \in R,$$
$$f(a.b) = f(a).' f(b) \quad \text{para todo } a, b \in R.$$

- Si f es inyectiva, se dice que f es un **monomorfismo**.
- Si f es sobreyectiva, se dice que f es un **epimorfismo**.
- Si f es biyectiva, se dice que f es un **isomorfismo**. En este caso se dice que los anillos R y R' son **isomorfos**.
- Si $R = R'$, se dice que f es un **endomorfismo**.
- Un endomorfismo biyectivo se le denomina un **automorfismo**.
- Si R y R' son dos anillos unitarios, diremos que $f : R \to R'$ es un **homomorfismos de anillos unitarios** si $f(1_R) = 1_{R'}$.

3.2 Proposición. Sean R y R' dos anillos, S un subanillo de R, S' un subanillo de R' y $f : R \to R'$ un homomorfismo de anillos. Entonces

(i) $f(S)$ es un subanillo de R'.

(ii) $f^{-1}(S') := \{r \in R |\ f(r) =\in S'\}$ es un subanillo de R.

En particular: $\mathrm{Ker}(f) := f^{-1}(0)$, llamado el **núcleo o Ker** de f, es un subanillo de R e $\mathrm{Im}(f) := f(R)$, llamada la **imagen** de f, es un subanillo de R' (cuando lleguemos a la estructura cociente en anillo veremos que $\mathrm{Ker}(f)$ tiene propiedades muy interesantes).

Es más:

- f es un monomorfismo si y sólo si $\mathrm{Ker}(f) = 0$.

– f es un epimorfismo si y sólo si $\mathrm{Im}(f) = R'$.

Nota: Si R y R' son dos anillos y $f : R \to R'$ un homomorfismo de anillos, $f(0) = 0$ y $f(-a) = -f(a)$. ¿Será cierto que $f(1) = 1'$? ¿Que ocurre entonces con los elementos inversibles de R?

3.3 Proposición. Sean R y R' dos anillos y $f : R \to R'$ un homomorfismo de anillos. Entonces:

(i) Si R es un anillo unitario, $\mathrm{Im}(f)$ es un anillo unitario con unidad $f(1)$.

(ii) Si a es un elemento inversible de R, $f(a)$ es un elemento inversible de $\mathrm{Im}(f)$.

(iii) Si f es sobreyectiva, entonces $f(1) = 1'$ y $f(a)$ es inversible para todo elemento inversible $a \in R$.

(iv) Si R y R' son unitarios y $f(1) = 1'$, $f(a)$ es inversible para todo elemento inversible $a \in R$.

Nota: Cada estructura que demos en algebra tendrá su homomorfismo asociado. Por ejemplo: si R es un subanillo de R', la inclusión de R en R' es un monomorfismo de anillos. Es más: si $f : R \to R'$ es un monomorfismo de anillos, entonces R es isomorfo a $\mathrm{Im}(f) \leq R'$, por lo que se puede considerar que R es un subanillo de R'.

3.4 Ejemplo. La aplicación nula y la identidad siempre son homomorfismos de anillos. Sea R un anillo y $a \in R$ una unidad. Entonces $f_a : R \to R$ definido por $f_a(x) = a^{-1}xa$ es un automorfismo de R.

En la siguiente proposición vamos a demostrar que todo anillo se puede "sumergir" en un anillo unitario:

3.5 Proposición. Sea R un anillo. Entonces $\mathbb{Z} \times R$ con suma y producto:

$$(\lambda, r) + (\mu, r') := (\lambda + \mu, r + r')$$
$$(\lambda, r).(\mu, r') := (\lambda\mu, \lambda r' + \mu r + r.r')$$

Tiene estructura de anillo unitario. Es más, la aplicación $\psi : R \to \mathbb{Z} \times R$ dada por $\psi(r) = (1, r)$ es un monomorfismo de anillos.

3.6 Def. Sea R un anillo. Se define la unitización de R, y se representa por R^1 como R, si éste ya es un anillo unitario o $\mathbb{Z} \times R$ caso de que R no sea unitario.

Nota: El conjunto de los homomorfismos entre dos anillos R y R' no tiene muy buenas propiedades, ya que ni la suma natural de aplicaciones es un homo-

morfismo: si consideramos la identidad en $\mathbb{Z}$, el anillo de los enteros, se tiene que $Id + Id$ no es un homomorfismo. ¿Cuales son los endomorfismos de $\mathbb{Z}$?

3.7 No obstante, dados dos grupos G y G' definimos $\mathrm{Hom}(G, G')$ como el conjunto de todos los homomorfismos de G en G'. Se tiene entonces que $\mathrm{Hom}(G, G')$ es un grupo con la suma usual: dados $f, g \in \mathrm{Hom}(G, G')$,

$$f + g : G \to G' \quad \text{definida por} \quad f + g(a) = f(a) + g(a).$$

Es mas, si G' es conmutativo, $\mathrm{Hom}(G, G')$ es un grupo abeliano y, si denotamos por $\mathrm{End}(G)$ al conjunto de todos los endomorfismos de un grupo abeliano G, $\mathrm{End}(G)$ con la suma usual y la composición de aplicaciones, $(\mathrm{End}(G), +, \circ)$ es un anillo unitario.

3.8 Teorema. Todo anillo es isomorfo a un subanillo de un anillo de endomorfismos de un cierto grupo abeliano.

Proof: Consideremos R^1 con su estructura de grupo abeliano. Veamos que la aplicación

$$\begin{array}{rccc} \Phi : & R & \to & \mathrm{End}(R^1) \\ & r & \mapsto & \Phi_r \end{array} \quad \text{definido por} \quad \Phi_r(r') = rr'$$

es un monomorfismos de anillos: dados r_1 y r_2 elementos de R,

– $\Phi_{r_1+r_2}(r') = (r_1 + r_2)r' = r_1r' + r_2r' = \Phi_{r_1}(r') + \Phi_{r_2}(r')$

– $\Phi_{r_1}\Phi_{r_2}(r') = r_1(r_2r') = (r_1r_2)r' = \Phi_{r_1r_2}(r')$

Lo que demuestra que es un homomorfismo de anillos. Por último, si $\Phi_r = 0$, $0 = \Phi_r(1) = r$, lo que demuestra que es inyectiva. ■

Nota: Este teorema nos dice como son todos los anillos. Al igual que el teorema de Cayley este resultado es poco útil.

3.9 Proposición. Sean $(R, +, .)$ y $(R', +', .')$ dos anillos y $f : R \to R'$ un isomorfismo de anillos. Entonces $f^{-1} : R' \to R$ también es un isomorfismo de anillos.

Nota: La aplicación inversa de un automorfismo $f : R \to R$ es precisamente el inverso de f en $\mathrm{End}(R)$ (considerado R únicamente como grupo abeliano).

4. LA CARACTERíSTICA DE UN ANILLO

4.1 Def. Sea R un anillo. Si existe el menor natural $n \in \mathbb{N}$ tal que

$a + \overset{n}{\cdots} + a = 0$ para todo $a \in R$ se dice que la característica de R es n. En caso contrario se dice que la característica de R es cero.

4.2 EJEMPLO. Para cada $n \in \mathbb{N}$, la característica de $\mathbb{Z}_n$ es n. La característica de $\mathbb{Z}$ es cero.

4.3 PROPOSICIÓN. Sea R un anillo unitario. Entonces la característica de R o es cero o el menor natural tal que $1 + \overset{n}{\cdots} + 1 = 0$ (o excluyente).

Nota: La característica de un anillo y de su unitización no tienen que coincidir. Es más, si R no es unitario la característica de R^1 es cero.

Nota: ¿Se te ocurre una nueva construcción para "sumergir" un anillo no unitario en un anillo unitario manteniendo la característica?

4.4 PROPOSICIÓN. La característica de un dominio de integridad es cero o un número primo.

5. EL PRODUCTO DIRECTO DE ANILLOS.

5.1 PROPOSICIÓN. Sea I un conjunto de indices y R_i, $i \in I$ una familia de anillos. Entonces $\Pi_{i\in I} R_i$ con su estructura habitual de grupo abeliano:

$$\Pi_{i\in I} R_i := \{(r_i)_{i\in I} \quad \text{con} \quad r_i \in R_i, \quad i \in I\}$$

$\star$ Con suma: $(r_i)_{i\in I} + (r'_i)_{i\in I} = (r_i + r'_i)_{i\in I}$

$\star$ y producto dado por componentes, $(r_i)_{i\in I}.(r'_i)_{i\in I} = (r_i.r'_i)_{i\in I}$

tiene estructura de anillo, llamado el **producto directo** de los R_i.

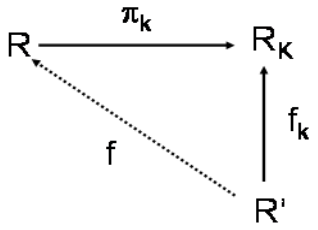
5.2 DEF:. Sean R_i, $i \in I$ una familia de anillos y sea $R = \Pi_{i\in I} R_i$ el producto directo de los R_i. Se define la **proyección "canónica"** de R en R_k, con $k \in I$, como:

$$\begin{array}{rccc} \pi_k : & R & \to & R_k \\ & (r_i)_{i\in I} & \mapsto & r_k. \end{array}$$

Es fácil ver que para cada $k \in I$, π_k es un epimorfismo de anillos.

5.3 PROPIEDAD FUNDAMENTAL DEL PRODUCTO DIRECTO DE ANILLOS.. Sean R_i, $i \in I$ una familia de anillos y sea $R = \Pi_{i\in I} R_i$ el producto directo de los R_i. Entonces para cada anillo R' y cada familia de homomorfismos de anillos

$f_i : R' \to R_i$ existe un único homomorfismo de anillos $f : R' \to R$ tal que para cada $k \in I$ el siguiente diagrama es conmutativo:



Es más, Si $\hat{R}$ es un anillo y $\rho_i : \hat{R} \to R_i$ son una familia de epimorfismos de anillos tales que para cada anillo R' y cada familia de homomorfismos de anillos $f_i : R' \to R_i$ existe un único homomorfismo de anillos $f : R' \to \hat{R}$ tal que para cada $k \in I$ el diagrama anterior es conmutativo, entonces $\hat{R}$ es isomorfo a $\Pi_{i\in I} R_i$.

Demo: Vamos a suponer en principio que existe este homomorfismo de anillos y demostremos que entonces sólo se puede definir de una manera, por lo que demostraremos que, caso de existir, es único. Luego veremos que esta solución verifica lo que queremos.

1-. Supongamos que existe $f : R' \to \Pi_{i\in I} R_i$ tales que $\pi_k \circ f = f_k$ tenemos entonces que dado $r' \in R'$, $f_k(r') = \pi_k(f(r'))$, por lo que la coordenada k-esima de $f(r')$ es $f_k(r')$. Así, $f(r') = (f_i(r'))_{i\in I}$.

2-. Comprobemos entonces que la aplicación $f : R' \to \Pi_{i\in I} R_i$ definido por $f(r') = (f_i(r'))_{i\in I}$ es un homomorfismo de anillos que verifica el enunciado:

$\star$ ¿Es homomorfismo de grupos?

$$\begin{aligned} f(r'_1 + r'_2) &= (f_i(r'_1 + r'_2))_{i\in I} = (f_i(r'_1) + f_i(r'_2))_{i\in I} = (f_i(r'_1))_{i\in I} + (f_i(r'_2))_{i\in I} \\ &= f(r'_1) + f(r'_2) \end{aligned}$$

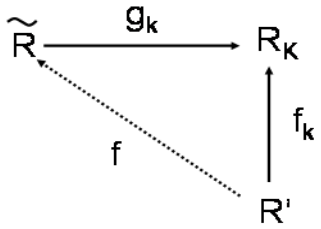
$\star$ ¿Es homomorfismo de anillos?

$$\begin{aligned} f(r'_1.r'_2) &= (f_i(r'_1.r'_2))_{i\in I} = (f_i(r'_1).f_i(r'_2))_{i\in I} = (f_i(r'_1))_{i\in I}.(f_i(r'_2))_{i\in I} \\ &= f(r'_1)f(r'_2) \end{aligned}$$

$\star$ ¿Hace conmutativo los diagramas? Pues claro

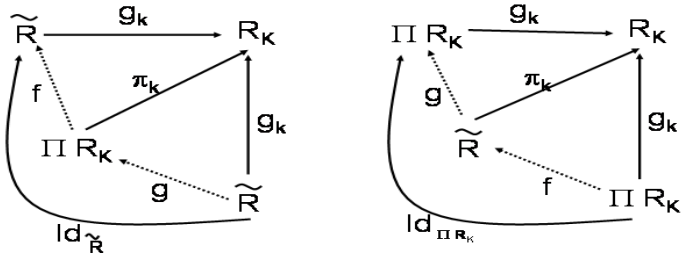
$$\pi_k \circ f(r') = \pi_k((f_i(r'))_{i\in I})) = f_k(r').$$

Veamos ahora que todo anillo con estas propiedades es isomorfo al producto cartesiano de los $\{R_i\}_{i\in I}$. Sea $\hat{R}$ un anillo y $g_i : \hat{R} \to R_i$ una familia de epimorfismos de anillos tales que para cada anillo R' y cada familia de homomorfismos de anillos $f_i : R' \to R_i$ existe un único homomorfismo de anillos $f : R' \to \hat{R}$ tal que para cada $k \in I$ el diagrama



es conmutativo.

Si consideramos ahora $R' = \Pi_{i\in I} R_i$ y $f_i = \Pi_i$ las proyecciones canónicas tenemos, aplicando varias veces esta propiedad fundamental, que:



En donde $f \circ g = Id_{\hat{R}}$ y $g \circ f = Id_{\Pi R_i}$ lo que demuestra que tanto f como g son isomorfismos, y por tanto $\hat{R}$ y $\Pi_{i\in I} R_i$ son anillos isomorfos.

6. LA SUMA DIRECTA DE ANILLOS.

6.1 PROPOSICIÓN. Sea I un conjunto de indices y R_i, $i \in I$ una familia de anillos. Entonces $\bigoplus_{i\in I} R_i$, con su estructura habitual de grupo abeliano:

$$\bigoplus_{i\in I} R_i = \{(r_i)_{i\in I} \in \Pi_{i\in I} R_i \mid r_i = 0 \quad \text{para casi todo } i\}$$

$\star$ Con suma: $(r_i)_{i\in I} + (r'_i)_{i\in I} = (r_i + r'_i)_{i\in I}$

$\star$ y producto dado por componentes, $(r_i)_{i\in I}.(r'_i)_{i\in I} = (r_i.r'_i)_{i\in I}$

tiene estructura de anillo, llamado la **suma directa externa** de los R_i.

Demo: Es claro que si sumo o multiplico dos elementos del producto con un número finito de coordenadas no nulas, obtengo un elemento con un número finito de coordenadas no nulas, ver [2.3, (2)] para el producto. Es decir, $\bigoplus_{i\in I} R_i$ es un subanillo del producto directo de anillos (ya que sabemos que es un subgrupo).

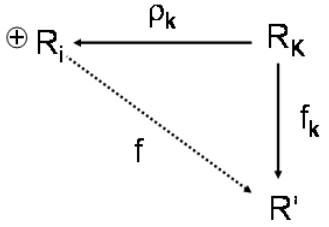
Nota: Si $\#I < \infty$ se tiene que la suma directa y el producto directo son isomorfos.

6.2 Def:. Sean $\{R_i\}_{i\in I}$ una familia de anillos y sea $\bigoplus_{i\in I} R_i$ la suma directa de éstos. Entonces para cada $k \in I$ se define la **inclusión canónica** de R_k en $\bigoplus_{i\in I} R_i$ y se representa por

$$\rho_k : R_k \to \bigoplus_{i\in I} R_i$$

como $\rho_k(r_k) = (x_i)_{i\in I}$ en donde $x_i = 0$ si $i \neq k$ y $x_k = r_k$. Es decir, el vector de $\Pi_{i\in I} R_i$ que tiene todas las coordenadas cero, salvo la k que vale r_k. Es claro que ρ_k es un monomorfismo de anillos.

6.3 Propiedad fundamental de la suma directa de anillos.. Sean $\{R_i\}_{i\in I}$ una familia de anillos y sea $\bigoplus_{i\in I} R_i$ la suma directa de éstos. Entonces para cada anillo R' y cada familia de homomorfismos de anillos $\{f_i\}_{i\in I}$ tales que $f_i : R_i \to R'$ verificando $f_s(x_s).f_r(x_r) = 0$ para todos $x_r \in R_r, x_s \in R_s$ con r, s dos elementos distintos de I, existe un único homomorfismo de anillos $f : \bigoplus_{i\in I} R_i \to R'$ tal que para cada $k \in I$ el siguiente diagrama es conmutativo:



Es más, Si $\hat{R}$ es un anillo y $g_i : R_i \to \hat{R}$ son una familia de monomorfismos de anillos tales que para cada anillo R' y cada familia de homomorfismos de anillos $f_i : R_i \to R'$ tales que $f_i : R_i \to R'$ verificando $f_s(x_s).f_r(x_r) = 0$ para todos $x_r \in R_r, x_s \in R_s$ con r, s dos elementos distintos de I, existe un único homomorfismo de anillos $f : \hat{R} \to R'$ tal que para cada $k \in I$ el diagrama anterior es conmutativo, entonces $\hat{R}$ es isomorfo a $\bigoplus_{i\in I} R_i$.

Demo: Vamos a suponer en principio que existe este homomorfismo de anillos y demostremos que entonces sólo se puede definir de una manera, por lo que demostraremos que, caso de existir, es único. Luego veremos que éste verifica lo que queremos.

1-. Supongamos que existe $f : \bigoplus_{i\in I} R_i \to R'$ tal que $f \circ \rho_k = f_k$ tenemos entonces que dado $r_k \in R_k$, $f_k(r_k) = f(\rho_k(r_k))$, por lo que $f((r_i)_{i\in I}) = f(\sum_{i\in I}(\rho_i(r_i))) = \sum_{i\in I} f_i(r_i)$. Observar que, aunque no lo parezca, por definición de suma directa está es una suma finita (en grupos no podemos sumar un número infinito de elementos).

2-. Comprobemos entonces que la aplicación $f : \bigoplus_{i\in I} R_i \to R'$ definido por $f((r_i)_{i\in I}) = \sum_{i\in I} f_i(r_i)$ es un homomorfismo de anillos que verifica el enunciado:

$\star$ ¿Es homomorfismo de grupos?

$$\begin{aligned} f((r_i)_{i\in I} + (r'_i)_{i\in I}) = f((r_i + r'_i)_{i\in I}) &= \sum_{i\in I} f_i(r_i + r'_i) \\ &= \sum_{i\in I} f_i(r_i) + \sum_{i\in I} f_i(r'_i) = f((r_i)_{i\in I}) + f((r'_i)_{i\in I}) \end{aligned}$$

$\star$ ¿va bien con el producto?

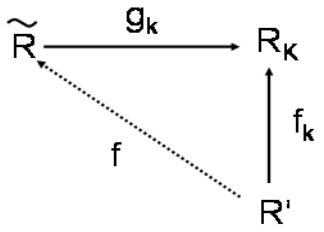
$$\begin{aligned} f((r_i)_{i\in I}.(r'_i)_{i\in I}) = f((r_i.r'_i)_{i\in I}) = \sum_{i\in I} f_i(r_i.r'_i) &= \sum_{i\in I} f_i(r_i).f_i(r'_i) \\ \overset{(*)}{=} \sum_{i\in I} f_i(r_i).\sum_{i\in I} f_i(r'_i) &= f((r_i)_{i\in I}).f((r'_i)_{i\in I}) \end{aligned}$$

Nota: Observar que la igualdad $(*)$ es cierta ya que $f_i(r_i).f_j(r_j) = 0$ para todo $i, j \in I$ con $i \neq j$.

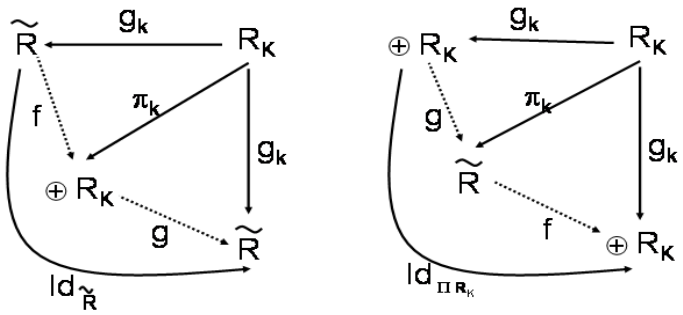
$\star$ ¿Hace conmutativo los diagramas? Pues claro

$$f \circ \rho_k(r_k) = f_k(r_k).$$

Veamos ahora que todo anillo con estas propiedades es isomorfo al producto cartesiano de los $\{R_i\}_{i\in I}$. Sea $\hat{R}$ un anillo y $g_i : R_i \to \hat{R}$ una familia de monomorfismos de anillos tales que para cada anillo R' y cada familia de homomorfismos de anillos $f_i : R_i \to R'$ existe un único homomorfismo de anillos $f : \hat{R} \to R'$ tal que para cada $k \in I$ el siguiente diagrama es conmutativo:



Si consideramos ahora $R' = \bigoplus_{i\in I} R_i$ y $f_i = \rho_i$ las inclusiones canónicas tenemos, aplicando varias veces esta propiedad fundamental:



En donde $g \circ f = Id_{\hat{R}}$ y $f \circ g = Id_{\bigoplus R_i}$ lo que demuestra que tanto f como g son isomorfismos, y por tanto $\hat{R}$ y $\bigoplus_{i\in I} R_i$ son anillos isomorfos.

7. EL ANILLO DE MATRICES

7.1 Proposición. Sea R un anillo y $n \in \mathbb{N}$. Entonces $\mathcal{M}_n(R)$ con su suma y producto habitual tiene estructura de anillo. Es más,

- $\mathcal{M}_n(R)$ es conmutativo si y sólo si R es conmutativo y $n = 1$.
- $\mathcal{M}_n(R)$ es un anillo de división si y sólo si R es un anillo de división y $n = 1$.
- $\mathcal{M}_n(R)$ es un cuerpo si y sólo si R es un cuerpo y $n = 1$.

8. EL ANILLO DE POLINOMIOS Y EL ANILLO DE SERIES FORMALES

8.1 Def. Sea R un anillo. Se define el anillo de series formales sobre R y se representa por $R[[X]]$ como:

$$R[X] := \{f : \mathbb{N} \to R\} \quad \text{supondremos en este caso que } 0 \in \mathbb{N}$$

con suma y producto dado por:

$$(f+g)(k) := f(k) + g(k)$$
$$(f.g)(k) := \sum_{i=0}^{k} f(i)g(k-i)$$

$$R[X] := \{f : \mathbb{N} \to R \mid f(i) = 0 \text{ casi para todo } i\}$$

9. HECHOS DESTACABLES:

- ⋆ Se han dado los anillos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, el anillo de congruencias módulo n (para n cualquier natural) y como ejemplo más abstracto $(\mathcal{P}(X), \triangle, \cap)$ para cualquier conjunto X.
- ⋆ Tenemos los subanillos de cualquier anillo dado.
- ⋆ Dado cualquier grupo abeliano G tenemos el anillo $\mathrm{End}(G)$.
- ⋆ Podemos construir el producto directo, así como la suma directa de una familia arbitraria de anillos.
- ⋆ Podemos construir el anillo de matrices de un anillo dado.

Bibliografía.

⋆ **J. B. Fraleigh**, "A First Course in Abstract Algebra". Addison-Wesley Publishing Company (1982).

⋆ **W. Keith Nicholson**, "Introduction to Abstract Algebra". J. Wesley & Sons Publishing Company (1999).