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.

Demo: 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.

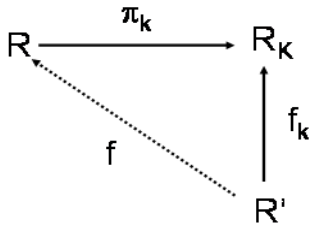
5.2 DEF:. Sean R_i, $i \in I$ una familia de anillos y sea $R = \Pi_{i\in I} R_i$ el producto directo de los R_i. Se define la **proyección "canónica"** de R en R_k, con $k \in I$, como:

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

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?

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

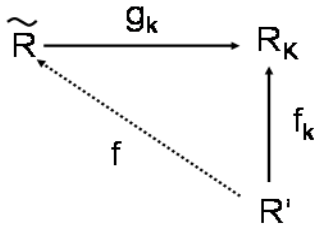
$\star$ ¿Es homomorfismo de anillos?

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

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

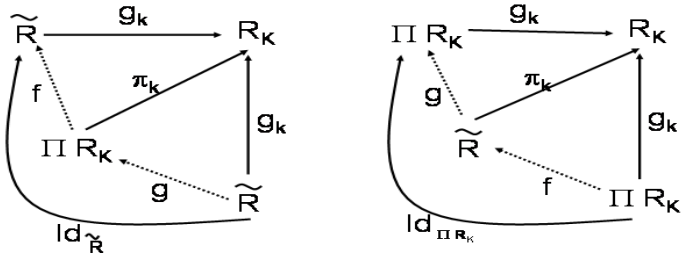
$$\pi_k \circ f(r') = \pi_k((f_i(r'))_{i\in I})) = f_k(r').$$

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).

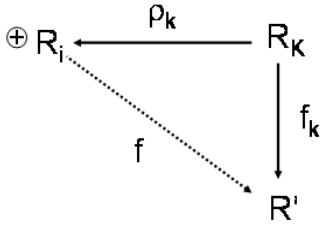
Nota: Si $\#I < \infty$ se tiene que la suma directa y el producto directo son isomorfos.

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?

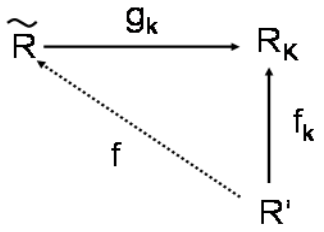
$$\begin{aligned} f((r_i)_{i\in I}.(r'_i)_{i\in I}) = f((r_i.r'_i)_{i\in I}) = \sum_{i\in I} f_i(r_i.r'_i) &= \sum_{i\in I} f_i(r_i).f_i(r'_i) \\ \overset{(*)}{=} \sum_{i\in I} f_i(r_i).\sum_{i\in I} f_i(r'_i) &= f((r_i)_{i\in I}).f((r'_i)_{i\in I}) \end{aligned}$$

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 $i \neq j$.

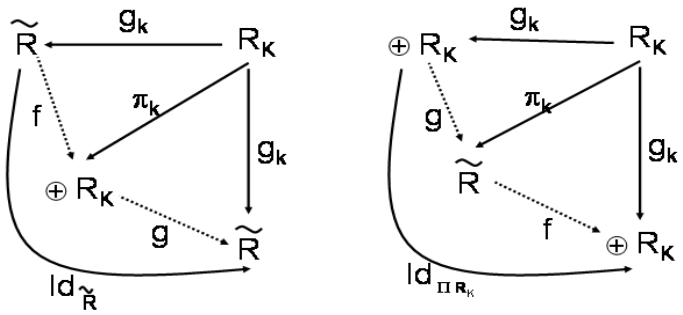
$\star$ ¿Hace conmutativo los diagramas? Pues claro

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

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).

TEMA 2.

1. INTRODUCCIÓN

En este tema vamos a estudiar más en profundidad los anillos de integridad: recordamos que dado un anillo R, un elemento no nulo $a \in R$ se dice que 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 **dominio de integridad** es un anillo conmutativo y unitario sin divisores de cero.

Como primer resultado obtendremos que los dominios de integridad son precisamente los anillo R en los que las ecuaciones $aX + b = 0$ y $Xa + b = 0$, con $a, b \in R$, caso de tener solución, está es única (esto no es más que otra forma de expresar las leyes de cancelación).

Observamos que los anillos de división son precisamente los anillos en los que estas ecuaciones tienen solución única.

Como último resultado de la sección demostraremos que todo dominio de integridad finito es cuerpo. Para finalizar el tema, demostraremos el Teorema (pequeño) de Fermat y una generalización de este, el teorema de Euler.

Nos harán falta los siguientes resultados (todos ellos visto en el primer cuatrimestre):

- ⋆ Toda aplicación inyectiva de un conjunto finito en si mismo es biyectiva.
- ⋆ Algoritmo de la división.
- ⋆ Nociones de divisibilidad. Los números primos.
- ⋆ Factorización de números enteros.
- ⋆ El máximo común divisor. El teorema de Bezout.
- ⋆ El mínimo común múltiplo.

2. PRIMERAS PROPIEDADES

2.1 Def. Diremos que un anillo R verifica la ley de cancelación por la izquierda si dados $a, b, c \in R$ con $c \neq 0$, $ca = cb$ entonces $a = b$. Diremos que un

anillo R verifica la ley de cancelación por la derecha si dados $a, b, c \in R$ con $c \neq 0$, $ac = bc$ entonces $a = b$.

2.2 Proposición. Sea R un anillo. Las siguientes condiciones son equivalentes:

(i) R verifica la ley de cancelación por la izquierda.

(ii) R no tiene divisores de cero por la derecha.

(iii) R no tiene divisores de cero por la izquierda.

(iv) R verifica la ley de cancelación por la derecha.

Nota: A partir de ahora hablaremos de anillos que verifican la ley de cancelación y anillos sin divisores de cero.

Nota: Todo dominio de integridad y todo anillo de división (en particular todo cuerpo) verifica la ley de cancelación.

2.3 Proposición. Sea R un anillo. Las siguientes condiciones son equivalentes:

(i) R no posee divisores de cero.

(ii) Para todo par de elementos $a, b \in R$ con $a \neq 0$, las ecuaciones $aX + b = 0$ y $Xa + b = 0$, si poseen solución, ésta es única.

2.4 Proposición. Sea R un anillo. Las siguientes condiciones son equivalentes:

(i) R es un anillo de división.

(ii) Para todo par de elementos $a, b \in R$ con $a \neq 0$, las ecuaciones $aX + b = 0$ y $Xa + b = 0$, poseen solución única.

2.5 Teorema. Todo dominio de integridad finito es cuerpo.

Demo: Sea D un dominio de integridad finito y $0 \neq a \in D$. Veamos que a es un elemento inversible de D. Consideremos la aplicación

$$\phi_a : D \to D \quad \text{definida por} \quad \phi_a(x) = ax.$$

Como D verifica la ley de cancelación por la izquierda, ϕ_a es una aplicación inyectiva y como D es finito, ϕ_a es sobreyectiva. Por tanto, existe $b \in D$ con $ab = 1$. Por último, como D es conmutativo $ab = ba = 1$ y a es inversible con inverso b. ■

Nota: Hemos demostrado un poco más:

⋆ Un anillo unitario y finito sin divisores de cero por la derecha (o por la izquierda) es un cuerpo: por la demostración anterior dado $a \in R$ existe $b \in R$ con $ab = 1$. Si repetimos el proceso para b, existe $c \in R$ con $bc = 1$. Pero entonces $a = a(bc) = (ab)c = c$ lo que demuestra que $a = c$ es un inverso para b en D, o lo que es lo mismo, que a es inversible con inverso b.

⋆ Si R es un anillo finito y unitario y $a \in R$ es un elemento que no es divisor de cero por la izquierda, entonces existe $b \in R$ con $ab = 1$. Si además a no es divisor de cero por la derecha, a es inversible (tomamos la aplicación $\rho_a(b) = ba$ y repetimos el argumento.

3. RECUERDO DEL PRIMER CUATRIMESTRE

Vamos a trabajar con $\mathbb{Z}$, el anillo de los enteros y su orden usual (recordamos que $(\mathbb{N}, \leq)$ es un conjunto bien ordenado: todo subconjunto no vacio de $\mathbb{N}$ posee un mínimo).

3.1 Algoritmo de la división. Dados $m, d \in \mathbb{Z}$, con $d > 0$, existen dos únicos elementos $c, r \in \mathbb{Z}$, con $0 \leq r < d$, tales que $m = cd + r$.

Nota: Se considera el conjunto $\{m - td \mid t \in \mathbb{Z} \text{ y } m - td > 0\}$. Se demuestra que es no vacio y se toma como r es mínimo en este conjunto. Posteriormente se demuestra la unicidad. ■

3.2 Def. Sean $n, m \in \mathbb{Z}$. Diremos que n divide a m (o que m es múltiplo de n) si existe $r \in \mathbb{Z}$ tal que $m = nr$.

3.3 Def. Sean $n, m \in \mathbb{Z}$ no nulos. Se define el máximo común divisor de m y n y se representa por $mcd(n, m)$ como un $d \in \mathbb{Z}$ tal que:

(i) $d > 0$.

(ii) d divide a n y a m.

(iii) Si a divide a n y a m, entonces a divide a d.

Nota: No hay que ser crédulo, hay que demostrar que este número siempre existe.

3.4 Def:. Sean $n, m \in \mathbb{Z}$ no nulos. Se define el mínimo común múltiplo de m y n y se representa por $MCM(n, m)$ como un $D \in \mathbb{Z}$ tal que:

(i) $D > 0$.

(ii) n y m dividen a D.

(iii) Si n y m dividen a a, entonces D divide a a.

Nota: Lo mismo de antes.

3.5 Teorema de Bezout. Sean $n, m \in \mathbb{Z}$ no nulos. Entonces existen $x, y \in \mathbb{Z}$ tales que $mcd(n, m) = xn + ym$.

3.6 Def. Se dice que $p \in \mathbb{Z}$ es un número primo si $p \geq 2$ y los únicos divisores de p son $\pm 1, \pm p$.

3.7 Teorema. Sea p un número primo de $\mathbb{Z}$ y sean $n_1, n_2, \ldots, n_k \in \mathbb{Z}$, con $k \in \mathbb{N}$. Entonces, si p divide a $\Pi_{i=1}^{k} n_i$, existe $s \in \{1, \ldots, n\}$ tal que p divide a n_s.

3.8 Teorema de factorización. Sea $n \in \mathbb{Z}$ con $n > 1$. Entonces n se puede escribir de forma única (salvo permutación) como producto de primos.

3.9 Teorema. Sean $n, m \in \mathbb{Z}$ no nulos. Entonces

$$mcd(n, m)MCM(n, m) = nm$$

4. ALGUNOS RESULTADOS EN TEORíA DE NÚMEROS

4.1 Proposición. Sea $n \in \mathbb{N}$. Entonces $\bar{a} \in \mathbb{Z}_n$ es divisor de cero si y sólo si $m.c.d(a, n) \neq 1$ si y solo si $\bar{a}$ no es inversible. Por tanto, $\mathbb{Z}_n$ es un cuerpo si y sólo si n es un número primo.

Demo: Sea $a \in \mathbb{Z}$. Supongamos en primer lugar que $mcd(n, a) = 1$. Entonces, por la igualdad de Bezout existen $x, y \in \mathbb{Z}$ tales que $xa + yn = 1$. Si miramos esta igualdad en $\mathbb{Z}_n$ lo que obtenemos es: $\bar{1} = \overline{xa + yn} = \bar{x}\bar{a} + \bar{y}\bar{n} = \bar{x}\bar{a}$ y por tanto $\bar{a}$ es un elemento inversible de $\mathbb{Z}_n$, por lo que no es divisor de cero. Si $mcd(a, n) = d \neq 1$, entonces $a = da'$, $n = dn'$ con $n' < n$. Por tanto $\bar{0} \neq \bar{n}' \in \mathbb{Z}_n$ y $\bar{a}\bar{n}' = \overline{da'n'} = \overline{a'n} = 0$, con lo que a es divisor de cero y no es inversible. ■

4.2 Teorema de Fermat. Sea p un número primo y $a \in \mathbb{Z}$ tal que p no divide a a. Entonces $a^{p-1} \equiv 1$ (mod p).

Demo: Consideremos $(\mathcal{U}(\mathbb{Z}_n),\ )$ el grupo de los elementos inversibles de $\mathbb{Z}_n$. Tenemos entonces, por un lado, que $\#U = p - 1$ y por otro que si p no divide a

a, $mcd(p,a) = 1$ y $a \in \mathcal{U}(\mathbb{Z}_n)$. luego por el Teorema de Lagrange, $\bar{a}^{p-1} = \bar{1}$ en $\mathcal{U}(\mathbb{Z}_n)$, o lo que es lo mismo, $a^{p-1} \equiv 1(mod(p))$. ■

4.3 Corolario. Sea $p \in \mathbb{Z}$ primo y $a \in \mathbb{Z}$. Entonces $a^p \equiv a$ (mod p).

4.4 Def. Se define la función de Euler como la aplicación $\phi : \mathbb{N} \to \mathbb{N}$ definida por

$$\phi(n) := \#\{a \in \mathbb{N} \mid a < n \text{ y } m.c.d(a,n) = 1\}$$

4.5 Teorema de Euler. Sea $a, n \in \mathbb{N}$ tales que $m.c.d(a,n) = 1$. Entonces $a^{\phi(n)} \equiv 1$ (mod n).

Demo: Análoga al teorema de Fermat. ■

5. 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).

TEMA 3.

1. INTRODUCCIÓN

El tema anterior ha tratado sobre los dominios de integridad, y muy particularmente sobre $\mathbb{Z}$, el anillo de los enteros. Es por todos conocidos la construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$:

– Definimos una relación de equivalencia en el conjunto de los pares $(a, b) \in \mathbb{Z}^* \times \mathbb{Z}$, en donde $\mathbb{Z}^*$ denota los enteros menos el cero. Diremos que dos pares (a, b) y (a', b') están relacionados si y sólo si $ab' = a'b$. La clase de equivalencia del elemento (a, b) se denota por $\frac{b}{a}$.

$$\mathbb{Q} := \{\frac{b}{a} \mid a, b \in \mathbb{Z},\ a \neq 0\}$$

– Definimos la suma y el producto en este conjunto como:

$$\text{La suma:} \qquad \frac{b}{a} + \frac{b'}{a'} := \frac{ba'+ab'}{aa'}.$$

$$\text{El producto:} \qquad \frac{b}{a} \times \frac{b'}{a'} := \frac{bb'}{aa'}.$$

Nos encontramos con que $(\mathbb{Q}, +, .)$ es el cuerpo de los racionales.

En este tema vamos a demostrar que esta construcción no es exclusiva de $\mathbb{Z}$, sino que cualquier dominio de integridad se "sumerge" de forma similar en un cuerpo.

2. CONSTRUCCIÓN DEL CUERPO DE FRACCIONES DE UN DOMINIO DE INTEGRIDAD

Sea D un dominio de integridad. Consideremos

$$D^* \times D := \{(a, b) \in D \times D \mid a \neq 0\}$$

2.1 Proposición. Sea D un dominio de integridad. Entonces, en $D^* \times D$ la relación, $(a, b) \cong (a', b')$ si y sólo si $ab' = a'b$, es de equivalencia.

Demo: Veamos que $\cong$ verifica las propiedades reflexiva, simétrica y transitiva:

$\star$ Reflexiva: sea $(a,b) \in D^* \times D$. Entonces $ab = ab$, con lo que $(a,b) \cong (a,b)$.

$\star$ Simétrica: Supongamos que $(a,b) \cong (a',b')$. Entonces, $ab' = a'b$ que directamente da $(a',b') \cong (a,b)$.

$\star$ Transitiva: Supongamos que $(a,b) \cong (a',b')$ y $(a',b') \cong (a'',b'')$. Entonces:

$$ab' = a'b \quad \text{y} \quad a'b'' = a''b'$$

si multiplicamos en la segunda igualdad por a y sustituimos ab' por $a'b$ (primera igualdad) obtenemos $aa'b'' = aa''b' = a''a'b$ (por lo que simplificando $0 \neq a'$, al verificar D la leyes de simplificación) $ab'' = a''b$, lo que nos demuestra que $(a,b) \cong (a'',b'')$. ■

Nota: El conjunto cociente $D^* \times D/\cong$ se denotará por $\mathcal{Q}(D)$. La clase de equivalencia de un elemento $(a,b) \in D^* \times D$ será denotada por $\frac{b}{a}$.

2.2 Teorema. Sea D un dominio de integridad. Entonces, en $\mathcal{Q}(D)$, las operaciones

$$\text{La suma:} \qquad \tfrac{b}{a} + \tfrac{b'}{a'} := \tfrac{ab'+ba'}{aa'}.$$

$$\text{El producto:} \qquad \tfrac{b}{a} \times \tfrac{b'}{a'} := \tfrac{bb'}{aa'}.$$

dotan a $\mathcal{Q}(D)$ de estructura de cuerpo (llamado el **cuerpo de fracciones** del dominio de integridad D). Es más, la aplicación $i : D \to \mathcal{Q}(D)$ definida por $i(d) = \frac{d}{1}$ es un monomorfismo de anillos unitarios.

Demo: Veamos que la suma anterior define una estructura de grupo abeliano en $\mathcal{Q}(D)$, para ello tendremos que demostrar:

(i) Que está bien definida (hace falta ver que el elemento $(aa', ab'+ba') \in D^* \times D$ y que esta suma no depende de los representantes.

(ii) Verifica las propiedades de grupo abeliano.

(i.1) Es claro que $aa' \neq 0$ ya que D es un dominio de integridad y $a \neq 0 \neq a'$.

(i.2) Veamos que esta suma no depende de los representantes. Supongamos que $(b,a) \cong (b_1,a_1)$ y que $(b',a') \cong (b'_1,a'_1)$. Tenemos entonces que:

$$ab_1 = a_1b \quad \text{y} \quad a'b'_1 = a'_1b' \qquad (H)$$

y queremos demostrar que $(aa', ab' + ba') \cong (a_1a'_1, a_1b'_1 + b_1a'_1)$, es decir:

$$aa'(a_1b'_1 + b_1a'_1) = a_1a'_1(ab' + ba')$$

$$\begin{aligned} aa'(a_1b'_1 + b_1a'_1) &= *^1 aa'a_1b'_1 + aa'b_1a'_1 = *^2 aa_1(a'b'_1) + (ab_1)a'a'_1 \\ &= *^3 aa_1(a'_1b') + (a_1b)a'a'_1 = *^4 a_1a'_1(ab' + ba') \end{aligned}$$

$*^1$ aplicando la propiedad asociativa y la distributiva.

$*^2$ aplicando la propiedad asociativa y la conmutativa.

$*^3$ aplicando las identidades de (H).

$*^4$ aplicando la propiedad asociativa, la conmutativa y la distributiva.

Luego la suma está bien definida en $\mathcal{Q}(D)$. Veamos ahora que $(\mathcal{Q}(D), +)$ tiene estructura de grupo abeliano. Antes veamos algunas propiedades útiles:

(P_1) Dado un elemento no nulo $c \in D$, para todo $\frac{b}{a} \in \mathcal{Q}(D)$, $\frac{b}{a} = \frac{cb}{ca}$.

(P_2) Dos elementos $\frac{b}{a}$, $\frac{b'}{a'}$ de $\mathcal{Q}(D)$ tienen representantes con el mismo denominador: $\frac{b}{a} = \frac{ba'}{aa'}$ y $\frac{b'}{a'} = \frac{ab'}{aa'}$.

(P_3) La suma de dos elementos $\frac{b}{a}$ y $\frac{c}{a}$ con el mismo "denominador" consiste en sumar "numeradores":

$$\frac{b}{a} + \frac{c}{a} = \frac{ba + ca}{a^2} = \frac{b + c}{a}$$

con estas tres propiedades, ya podemos demostrar fácilmente que $(\mathcal{Q}(D), +)$ tiene estructura de grupo abeliano. Por P_3 voy a tomar, cuando me sea de interés, "fracciones" con el mismo denominador"

(ii.1) Asociativa: sean $\frac{b_1}{a}, \frac{b_2}{a}, \frac{b_3}{a} \in \mathcal{Q}(D)$. Entonces:

$$\left(\frac{b_1}{a} + \frac{b_2}{a}\right) + \frac{b_3}{a} = \frac{b_1 + b_2}{a} + \frac{b_3}{a} = \frac{b_1 + b_2 + b_3}{a} = \frac{b_1}{a} + \frac{b_2 + b_3}{a} = \frac{b_1}{a} + \left(\frac{b_2}{a} + \frac{b_3}{a}\right)$$

(ii.2) Conmutativa: sean $\frac{b_1}{a}, \frac{b_2}{a} \in \mathcal{Q}(D)$. Entonces:

$$\frac{b_1}{a} + \frac{b_2}{a} = \frac{b_1 + b_2}{a} = \frac{b_2 + b_1}{a} = \frac{b_2}{a} + \frac{b_1}{a}$$

(ii.3) Neutro: $0 = \frac{0}{1} \in \mathcal{Q}(D)$.

(ii.4) Opuesto: dado $\frac{b}{a} \in \mathcal{Q}(D)$, $\frac{-b}{a}$ es su opuesto, ya que $\frac{b}{a} + \frac{-b}{a} = \frac{0}{a} = 0$.

Nota: El neutro de la suma es cualquier elemento de la forma $\frac{0}{a}$ con $a \in D^*$.

Veamos ahora la propiedad asociativa del producto y las distributivas:

(iii.1) Asociativa: sean $\frac{b_1}{a_1}, \frac{b_2}{a_2}, \frac{b_3}{a_3} \in \mathcal{Q}(D)$. Entonces:

$$\left(\frac{b_1}{a_1}\frac{b_2}{a_2}\right)\frac{b_3}{a_3} = \frac{b_1b_2}{a_1a_2}\frac{b_3}{a_3} = \frac{b_1b_2b_3}{a_1a_2a_3} = \frac{b_1}{a_1}\frac{b_2b_3}{a_2a_3} = \frac{b_1}{a_1}\left(\frac{b_2}{a_2}\frac{b_3}{a_3}\right)$$

(iii.2) Conmutativa: sean $\frac{b_1}{a_1}, \frac{b_2}{a_2} \in \mathcal{Q}(D)$. Entonces:

$$\frac{b_1}{a_1}\frac{b_2}{a_2} = \frac{b_1b_2}{a_1a_2} = \frac{b_2b_1}{a_1a_2} = \frac{b_2}{a_2}\frac{b_1}{a_1}$$

(iv) Distributiva: demostramos sólo la distributiva por un lado, ya que hemos demostrado que el producto es conmutativo. Sean $\frac{b_1}{a}, \frac{b_2}{a}, \frac{b_3}{a} \in \mathcal{Q}(D)$. Entonces:

$$\begin{aligned}\left(\frac{b_1}{a} + \frac{b_2}{a}\right)\frac{b_3}{a} &= \frac{b_1 + b_2}{a}\frac{b_3}{a} = \frac{(b_1 + b_2)b_3}{a^2} = \frac{b_1b_3 + b_2b_3}{a^2} \\ &= \frac{b_1b_3}{a^2} + \frac{b_2b_3}{a^2} = \frac{b_1}{a}\frac{b_3}{a} + \frac{b_2}{a}\frac{b_3}{a}\end{aligned}$$

Por último demostremos que $\mathcal{Q}(D)$ es un cuerpo, es decir, que es un anillo unitario y que todo elemento no nulo tiene inverso.

(v.1) Elemento neutro: el elemento $\frac{1}{1}$ es el elemento neutro de la suma.

Nota: por la propiedad P_1, $\frac{1}{1} = \frac{a}{a}$ para todo $a \in D^*$.

(v.2) Sea $\frac{b}{a}$ un elemento no nulo de $\mathcal{Q}(D)$. Por lo anterior, $b \neq 0$ y por tanto, $\frac{b}{a}$ es el inverso:

$$\frac{b}{a}\frac{a}{b} = \frac{ba}{ab} = \frac{1}{1}$$

Veamos que la aplicación $i : D \to \mathcal{Q}(D)$, definida por $i(d) := \frac{d}{1}$, es un monomorfismo de anillos.

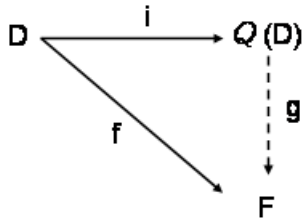
$$\begin{aligned}i(b_1 + b_2) &= \frac{b_1 + b_2}{1} = \frac{b_1}{1} + \frac{b_2}{1} = i(b_1) + i(b_2) \\ i(b_1b_2) &= \frac{b_1b_2}{1} = \frac{b_1}{1}\frac{b_2}{1} = i(b_1)i(b_2)\end{aligned}$$

Por último si $i(b) = 0$, entonces $\frac{b}{1} = \frac{0}{1}$ por lo que $b1 = 0.1 = 0$ y $b = 0$, es decir, i es una aplicación inyectiva. ■

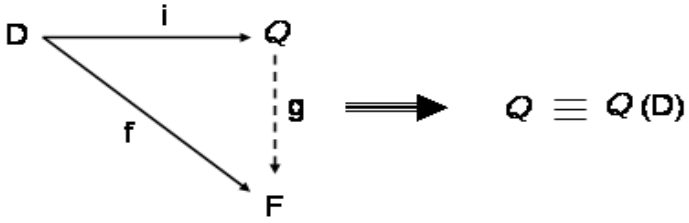
2.3 Corolario. Un anillo R es un dominio de integridad si y sólo si es subanillo de un cuerpo.

La segunda parte importante del cuerpo de fracciones $\mathcal{Q}(D)$ de un dominio de integridad D es que es el cuerpo "más pequeño" que contiene a D. Naturalmente la noción de "ser más pequeño que" es:

2.4 Teorema. Sea D un dominio de integridad, F un cuerpo y $f : D \to F$ un monomorfismo de anillos. Entonces existe un único monomorfismo de anillos $g : \mathcal{Q}(D) \to F$ que hace conmutativo el diagrama.



Es más, si Q es un cuerpo tal que existe un monomorfismo de anillos $i : D \to Q$ y tal que para cada cuerpo F y cada monomorfismo de anillos $f : D \to F$, existe un único monomorfismo de anillos $g : Q \to F$ que hace conmutativo el diagrama. Se tiene que Q es isomorfo al cuerpo de fracciones de D.



3. GENERALIZACIONES

En todo este tema hemos partido de D, un dominio de integridad, pero ¿nos hacia falta tanto?

3.1 UNIDAD. Si nos fijamos bien en la demostraciones que hemos hecho, ¿donde se usa que D sea unitario?

En la proposición (2.1) no se usa el carácter unitario: la relación $(a, b) \cong (a', b')$ si y sólo si $ab' = a'b$ es de equivalencia, sea D unitario o no.

El Teorema (2.2) demuestra que el conjunto cociente, $\mathcal{Q}(D)$ con las operaciones definidas tiene estructura de anillo (aquí no hace falta la unidad. Para demostrar que $\mathcal{Q}(D)$ es un cuerpo (luego unitario), parece ser que sí. No obstante, dado $0 \neq a \in D$, $\frac{a}{a}$ es la unidad de $\mathcal{Q}(D)$ y el inverso de un elemento no nulo $\frac{b}{a}$ sigue siendo $\frac{a}{b}$. Por lo que la unidad de D, en realidad, no ha hecho falta.

Si nos damos cuenta, los últimos teoremas tampoco hacen uso de que D tiene un elemento unitario.

3.2 DIVISORES DE CERO. Aquí la cosa se complica algo más. Pero en realidad dado un anillo R, si definimos el conjunto $Z(R)$ como:

$$Z(R) = \{a \in R \mid ax = xa \quad \text{para todo} \quad x \in R\}$$

y no hay divisores de cero R contenidos en $Z(R)$. Se puede dar una construcción idéntica en la anterior, en la que se obtiene un anillo denotado por $Z^{-1}R$ y que tiene la propiedad que todo elemento no nulo de $Z(R)$ es inversible en $Z^{-1}R$.

Observar que si D es un dominio de integridad $Z(D) = D$.

4. 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).

TEMA 4.

1. INTRODUCCIÓN

En este capitulo vamos a introducir la estructura cociente. En el cuatrimestre anterior se ha estudiado esta noción en el contexto de grupos, apareciendo la noción de subgrupo normal: Dado un grupo G y un subgrupo N, se podia construir la estructura cociente Q/N si y sólo si N era subgrupo normal de G.

Dado un anillo R y una relación de equivalencia $\cong$ en R vamos a definir una estructura de anillo en el conjunto cociente $R/\cong$, en donde la suma y el producto queden definidos por:

$$\bar{x} + \bar{y} := \overline{x+y}$$
$$\bar{x}\bar{y} := \overline{xy}$$

Nota: Lo cual, al igual que en el caso de grupos, significa "buscar" cuales son las relaciones de equivalencia compatibles con las operaciones del anillo.

Si consideramos G un grupo con elemento neutro e y $\cong$ una relación en G que de estructura de grupo al cociente, tenemos:

– La clase del elemento neutro $[e]$, es cerrada para la suma: $[e] + [e] = [e]$.

– Si $x \in [e]$, $x^{-1} \in [e]$: si $x \in [e]$, $[e] = [e][e] = [x][x^{-1}] = [e][x^{-1}] = [x^{-1}]$. Por lo que $[e]$ resulta ser un subgrupo.

– $[e]$ es un subgrupo normal de G: dado $x \in [e]$ e $y \in G$, $[yxy^{-1}] = [y][x][y^{-1}] = [y][e][y^{-1}] = [y][y^{-1}] = [e]$. Por lo que $yxy^{-1} \in [e]$.

Por último, si definimos la relación: dados $x, y \in G$ diremos que $x \equiv y$ si y solo si $xy^{-1} \in [e]$. Resulta que la clases de equivalencia de $\cong$ y $\equiv$ coinciden, por lo que son la misma relación de equivalencia. Así, se introduce la estructura cociente de un grupo G respecto de un cierto subgrupo normal N.

Veamos que sucede en teoría de anillos.

2. IDEALES DE UN ANILLO

Sea R un anillo y $\cong$ una relación de equivalencia en R. Queremos definir una estructura de anillo en el conjunto cociente $R/\cong$, en donde la suma y el producto

queden definidos por:

$$\bar{x} + \bar{y} := \overline{x + y}$$
$$\bar{x}\bar{y} := \overline{xy}$$

Tenemos que $(R/\cong, +)$ va a tener estructura de grupo, por lo que las únicas posibles relaciones de equivalencia vienen dadas a partir de subgrupos normales de $(R, +)$.

Nota: Como $(R, +)$ es un grupo abeliano, cualquier subgrupo de R es un subgrupo normal.

Sea R un anillo, I un subgrupo de R y $\cong$ la relación $x \cong y$ si y solo si $x - y \in I$. Supongamos que $R/\cong$ tiene estructura de anillo. entonces:

– Dado $x \in R$, $y \in I$, $[x][y] = [0][y] = [0]$, $[y][x] = [y][0] = [0]$. Por lo que para todo $x \in R$, $y \in I$, $xy, yx \in I$.

Veamos que ésta es la condición que nos faltaba.

2.1 Def. Sea R un anillo. Se dice que $I \subset R$ es un **ideal** de R si I es un subanillo de R tal que para todo $x \in R$, $y \in I$, $xy, yx \in I$.

2.2 Ejemplos. — Sea R un anillo, entonces R y $\{0\}$ son siempre ideales de R (llamados triviales).

— Sea $\mathbb{Z}$ el anillo de los enteros. Entonces para cada $n \in \mathbb{N}$ el conjunto $n\mathbb{Z}$ es un ideal de $\mathbb{Z}$.

2.3 Proposición. Sea R un anillo e I un ideal de R. Entonces si I contiene un elemento inversible de R, $I = R$. Por tanto los únicos ideales de un anillo de división son los triviales.

2.4 Teorema. Sea R un anillo e I un ideal de R. Entonces:

(i) La relación $x \cong y$ si y solo si $x - y \in I$ es de equivalencia.

(ii) $(R/\cong, +,)$ con las operaciones

$$\bar{x} + \bar{y} := \overline{x + y}$$
$$\bar{x}\bar{y} := \overline{xy}$$

tiene estructura de anillo.

El anillo anterior se denota por R/I y se llama el **anillo cociente de** R **sobre** I.

Asociado a cada estructura hay asociado un homomorfismo, en el caso de anillos de cocientes no iba a ser menos:

2.5 Def. Sea R un anillo y I un ideal de R. Entonces la aplicación $\pi : R \to R/I$ definida por $\pi(r) = [r]$ es un epimorfismo de anillos (llamado el epimorfismo de **proyección** de R en R/I).

2.6 Teorema (Propiedad fundamental del cociente). Sean R y R' dos anillos y $f : R \to R'$ un homomorfismo de anillos. Sea I un ideal de R tal que $I \subset \mathrm{Ker}(f)$. Entonces la aplicación $\bar{f} : R/I \to R'$ definida por $\bar{f}(\bar{x}) := f(x)$ es un homomorfismo de anillos.

2.7 Teorema (primer teorema de Isomorfía). Sean R y R' dos anillos y $f : R \to R'$ un homomorfismo de anillos. Entonces:

(i) $\mathrm{Ker}(f) \lhd R$.

(ii) $R/\mathrm{Ker}(f) \cong Im(f)$. Es más, la aplicación $\bar{f} : R/\mathrm{Ker}(f) \to Im(f)$ definida por $\bar{f}([x]) := f(x)$ es un isomorfismo de anillos.

2.8 Ejemplo. Sea $\mathbb{Z}$ el anillo de los enteros y $n \in \mathbb{N}$. Entonces $\mathbb{Z}/n\mathbb{Z} \equiv \mathbb{Z}_n$.

2.9 def. Sea R un anillo. Se dice que I es un ideal por la izquierda de R y se representa por $I \lhd_l R$ si I es un subanillo de R tal que para todo $x \in R$, $y \in I$, $xy \in I$. Se dice que I es un ideal por la derecha de R y se representa por $I \lhd_r R$ si I es un subanillo de R tal que para todo $x \in R$, $y \in I$, $yx \in I$.

Nos va a interesar construir ideales a partir de elementos. El siguiente teorema nos dice como.

2.10 Proposición. Sea R un anillo y $x \in R$. Entonces:

(i) $Rx = \{ax \mid a \in R\}$ es un ideal por la izquierda de R. Si R es unitario $x \in Rx$.

(ii) $Rx + \mathbb{Z}x$ es un ideal por la izquierda de R que contiene a x. Es más, éste es es el ideal por la izquierda más pequeño de R que contiene a x.

(iii) $xR = \{xa \mid a \in R\}$ es un ideal por la derecha de R. Si R es unitario $x \in xR$.

(iv) $xR + \mathbb{Z}x$ es un ideal por la derecha de R que contiene a x. Es más, éste es es el ideal por la derecha más pequeño de R que contiene a x.

(v) $RxR = \{\sum_{finita} a_i x b_i \mid a_i, b_i \in R\}$ es un ideal de R. Si R es unitario, $x \in RxR$.

(vi) $RxR + Rx + xR + \mathbb{Z}x$ es un ideal de R que contiene a x. Es más, éste es es el ideal más pequeño de R que contiene a x.

2.11 Proposición. Sea R un anillo y I_1, I_2 dos ideales (ideales por la izquierda, por la derecha) de R. Entonces:

(i) $I_1 \cap I_2$ es un ideal (ideal por la izquierda, por la derecha) de R.

(ii) $I_1 + I_2$ es un ideal (ideal por la izquierda, por la derecha) de R.

(iii) $I_1 I_2 := \{\sum y_i y_i' \mid y_i \in I_1, y_i' \in I_2\}$ es un ideal (ideal por la izquierda, por la derecha) de R.

Es más, si I_1, I_2 son ideales de R, entonces $I_1 I_2 \subset I_1 \cap I_2 \subset I_1 + I_2$.

2.12 Teorema. Sea R un anillo e I_1, I_2 dos ideales de R. Entonces:

(i) I_1, I_2 son ideales de $I_1 + I_2$ y $I_1 \cap I_2$ es ideal tanto de I_1 como de I_2.

(ii) $I_1 + I_2/I_1 \cong I_2/\cap(I_1 \cap I_2)$.

2.13 Teorema. Sea R un anillo e $I_1 \subset I_2$ dos ideales de R. Entonces:

(i) I_1/I_2 es un ideal de R/I_2.

(ii) $(R/I_2)/(I_1/I_2) \cong R/I_1$.

3. SUBCUERPO PRIMO

En esta sección vamos a ver que todo anillo de división Δ contiene como subanillo a $\mathbb{Z}_p$ o a $\mathbb{Q}$. Más precisamente:

3.1 Teorema. Sea $\mathbb{F}$ un cuerpo. Entonces:

(i) Si $\mathbb{F}$ tiene característica cero, $\mathbb{Q} \subset \mathbb{F}$.

(i) Si $\mathbb{F}$ tiene característica p, $\mathbb{Z}_p \subset \mathbb{F}$.

A $\mathbb{Q}$ o $\mathbb{Z}_p$, con p un número primo, se les denomina los subcuerpos primos.

Demo: Sea la aplicación $f : \mathbb{Z} \to \mathbb{F}$ definida por $f(n) = 1 + \overset{n}{\cdots} + 1 = n1$. Claramente, f es un homomorfismo de anillos, es más:

$\star$ Si la característica de Δ es 0, f es un monomorfismo de anillos, por lo que aplicado la propiedad fundamental del cuerpo de fracciones de un dominio de integridad, existe $\bar{f} : \mathbb{Q} \to \mathbb{F}$ un monomorfismo de anillos, por lo que se puede considerar $\mathbb{Q}$ contenido en $\mathbb{F}$.

$\star$ Si la característica de $\mathbb{F}$ es un número p, (que sabemos que es un número primo), $\mathrm{Ker}(f) = p\mathbb{Z}$ y por el primer teorema de Isomorfía

$$\mathbb{Z}_p \cong \mathbb{Z}/\mathrm{Ker}(f) \cong \mathrm{Im}(f) \subset \mathbb{F}.$$

lo que nos demuestra el teorema. ■

4. IDEALES PRIMOS, IDEALES MAXIMALES

Los dos últimos resultados importantes de este tema se van a centrar en teoría de anillos unitarios. No obstante las definiciones se harán de forma general.

4.1 Def. Sea R un anillo. Se dice que un ideal I de R es maximal si $I \neq R$ y dado cualquier ideal J de R tal que $I \subset J \subset R$ se tiene que $J = I$ o $J = R$.

4.2 Teorema. Un ideal I de un anillo conmutativo y unitario R es maximal si y solo si el anillo cociente R/I es un cuerpo.

Demo: Supongamos que R/I es un cuerpo y sea J un ideal de R distinto de I con $I \subset J$. Entonces, dado $x \in J - I$, $\bar{0} \neq \bar{x} \in R/I$ y como R/I es un cuerpo, existe $\bar{z} \in R/I$ tal que $\overline{xz} = \bar{1}$. Por tanto, $xz - 1 = y \in I$ y así, $1 = xz - y \in J$, ya que $xz \in J$ y $y \in I \subset J$. Luego $J = R$ al contener a 1.

Supongamos que I es un ideal maximal de R y sea $\bar{0} \neq \bar{x} \in R/I$. Tenemos entonces que $x \notin I$. Por otro lado, Rx es un ideal de R que contiene a x (ya que R es conmutativo y unitario) y por tanto $I + Rx$ es un ideal de R que contiene a I y a x, por lo que, por la maximalidad de I, $I + Rx = R$. Así, existe $y \in I$ y $z \in R$ con $y + zx = 1$ o lo que es lo mismo, $\bar{x}\bar{z} = \bar{1}$ en R/I. Luego R/I es un anillo conmutativo y unitario en donde todo elemento no nulo tiene inverso, R/I es un cuerpo. ■

4.3 Def:. Se dice que un anillo R es simple si los únicos ideales que posee son los triviales.

Ya sabemos que los anillos de división y en particular los cuerpos son anillos simples. En el caso de anillos conmutativos y unitarios se tiene el recíproco:

4.4 Corolario. Un anillo conmutativo y unitario R es un cuerpo si y sólo si sólo posee los ideales triviales.

Demo: Si R es un cuerpo, R sólo tiene los ideales triviales. Si R es un anillo conmutativo y unitario que sólo posee los ideales triviales, $\{0\}$ es un ideal maximal de R y por tanto, $R/\{0\} \cong R$ es un cuerpo. ■

Hay ejemplos de anillos simples que no son de división:

4.5 Teorema. Sea R un anillo y $n \in \mathbb{N}$. Entonces $\mathcal{I}$ es un ideal de $\mathcal{M}_n(R)$ si y solo si $\mathcal{I} = \mathcal{M}_n(I)$ para I un ideal de R.

Demo: Sea I un ideal de R. Entonces $\mathcal{M}_n(I)$ es un ideal de $\mathcal{M}_n(R)$:

⋆ $(\mathcal{M}_n(I), +)$ es un grupo abeliano: dados $(y_{ij})_{ij=1}^n, (y'_{ij})_{ij=1}^n \in \mathcal{M}_n(I)$,

– $(y_{ij})_{ij=1}^n + (y'_{ij})_{ij=1}^n = (y_{ij} + y'_{ij})_{ij=1}^n \in \mathcal{M}_n(I)$.

– $(0_{ij})_{ij=1}^n \in \mathcal{M}_n(I)$

– El opuesto de $(y_{ij})_{ij=1}^n$ es $(-y_{ij})_{ij=1}^n \in \mathcal{M}_n(I)$

⋆ Veamos que es un ideal: dados $(y_{ij})_{ij=1}^n \in \mathcal{M}_n(I)$ y $(x_{ij})_{ij=1}^n \in \mathcal{M}_n(R)$,

– $(x_{ij})_{ij=1}^n (y_{ij})_{ij=1}^n = (\sum_{k=1}^n x_{ik}y_{kj})_{ij=1}^n \in \mathcal{M}_n(I)$, ya que $x_{ik}y_{kj} \in I$ para cualesquiera $i, j, k \in \{1, 2, \cdots, n\}$.

– $(y_{ij})_{ij=1}^n (x_{ij})_{ij=1}^n = (\sum_{k=1}^n y_{ik}x_{kj})_{ij=1}^n \in \mathcal{M}_n(I)$, ya que $y_{ik}yx_{kj} \in I$ para cualesquiera $i, j, k \in \{1, 2, \cdots, n\}$.

Sea ahora $\mathcal{I}$ un ideal de $\mathcal{M}_n(R)$. Veamos que existe un ideal I de R tal que $\mathcal{I} = \mathcal{M}_n(I)$: denotemos por e_{ij} la matriz de $\mathcal{M}_n(R)$ que tiene un uno en el lugar ij y ceros en el resto.

⋆ Dada una matriz $A = (a_{ij})_{ij=1}^n \in \mathcal{M}_n(R)$, $A = \sum_{ij=1}^n e_{ii}Ae_{jj}$: sólo hay que darse cuenta que $e_{ii}Ae_{jj}$ es la matriz que tiene a a_{ij} en el lugar ij y ceros en el resto.

⋆ Si $Y = (x_{ij})_{ij=1}^n \in \mathcal{I}$, y considero $x_{rs} \in R$ la coordenadas rs de esta matriz, entonces la matriz A que tiene a x_{rs} en el lugar $r's'$ y ceros en el resto pertenece a $\mathcal{I}$: solo hay que darse cuenta que $A = e_{r'r}(x_{rs})_{ij=1}^n e_{ss'}$.

Consideremos la aplicación

$$\pi_{11} : \mathcal{M}_n(R) \to R \quad \text{definida por} \quad \pi((x_{ij})_{ij=1}^n) = x_{11}.$$

y sea $I = \pi_{11}(\mathcal{I})$ (el conjunto de las coordenadas 11 de cada matriz de $\mathcal{I}$).

Veamos que $\mathcal{I} \subset \mathcal{M}_n(I)$: dado $Y \in \mathcal{I}$, por la propiedad segunda, cada coordenada de Y pertenece a I.

Veamos que $\mathcal{M}_n(I) \subset \mathcal{I}$: dada una matriz $A \in \mathcal{M}_n(I)$, por la propiedad primera, $A = \sum_{ij=1}^{n} e_{ii}Ae_{jj}$ y por la propiedad segunda cada matriz $e_{ii}Ae_{jj} \in \mathcal{I}$. ■

4.6 Corolario. Sea R un anillo simple y unitario. Entonces para cada $n \in \mathbb{N}$, $\mathcal{M}_n(R)$ es un anillo simple y unitario. En particular $\mathcal{M}_n(\mathbb{F})$ es simple (y no es un cuerpo o un anillo de división) para cada cuerpo $\mathbb{F}$.

En particular $\mathcal{M}_n(\mathbb{F})$ es simple (y no es un cuerpo o un anillo de división) para cada cuerpo $\mathbb{F}$.

4.7 Def. Sea R un anillo. Se dice que un ideal I de R es primo si $I \neq R$ y para todos $x, y \in R$ tales que $xy \in I$ se tiene que $x \in I$ o $y \in I$.

4.8 Teorema. Un ideal I de un anillo conmutativo y unitario R es primo si y solo si el anillo cociente R/I es un dominio de integridad.

Demo: Supongamos que el anillo cociente R/I es un dominio de integridad y sean $x, y \in R$ con $xy \in I$. Tenemos entonces que $\overline{xy} = \bar{0}$ en el dominio de integridad R/I por lo que o $\bar{x} = \bar{0}$, y así $x \in I$ o $\bar{y} = \bar{0}$, y así $y \in I$.

Supongamos que I es un ideal primo de R. Veamos que el anillo cociente R/I es un dominio de integridad. Sean $\bar{x}, \bar{y} \in R/I$, con $\bar{x}\bar{y} = \bar{0}$. Entonces $\overline{xy} = \bar{0}$ y por tanto $xy \in I$. Luego $x \in I$, y así $\bar{x} = \bar{0}$ o $y \in I$, y así $\bar{y} = \bar{0}$. Así, R/I es un anillo conmutativo y unitario sin divisores de cero. ■

4.9 Corolario. Sea R un anillo conmutativo y unitario. Entonces todo ideal maximal de R es primo.

Demo: Si I es un ideal maximal de R, R/I es un cuerpo y por tanto un dominio de integridad, lo que implica que I es un ideal primo. ■

5. 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).

TEMA 6.

1. INTRODUCCIÓN

Hemos estudiado a lo largo del curso dos anillos de integridad: $\mathbb{Z}$, el anillo de los enteros, y $\mathbb{F}[X]$ con $\mathbb{F}$ un cuerpo, el anillo de polinomios con coeficientes en un cuerpo, que además de ser dominios de integridad tienen una propiedad muy curiosa: todo elemento se escribe "de forma única" como producto de "primos". En este tema vamos a estudiar dominios de integridad con esta propiedad, los dominios de factorización única.

2. DEFINICIONES

2.1 Def. Sea D un dominio de integridad. Se dice que $u \in D$ es una unidad si u es un elemento inversible de D. Dados $a, b \in D$. Se dice que a divide a b y se representa $a|b$ si existe $c \in D$ tal que $b = ac$.

2.2 Propiedades. Sea D un dominio de integridad y sean $a, b, c \in D$. Entonces:

(i) $a|a$.

(ii) Si $a|b$ y $b|c$, entonces $a|c$.

(iii) Si $a|b$ y $a|c$, entonces $a|xb + yc$ para todo $x, y \in \mathbb{Z}$.

2.3 Proposición. Sea D un dominio de integridad y sean $a, b \in D$. Las siguientes condiciones son equivalentes:

(i) $a|b$ y $b|a$.

(ii) Existe $u \in D$ una unidad tal que $a = ub$.

(iii) $Da = Db$ (El ideal generado por a coincide con el ideal generado por b).

Si a, b verifican las condiciones anteriores, se dice que a y b son asociados y se representa por $a \sim b$.

2.4 Corolario. Sea D un dominio de integridad. Entonces la relación $\sim$ es de equivalencia.

2.5 Def. Sea D un dominio de integridad. Se dice que un elemento $p \in D$ es irreducible si:

(i) p no es una unidad ni es cero.

(ii) Si $p = ab$ con $a, b \in D$, entonces a o b es una unidad de D.

2.6 Ejemplo. Los números primos de $\mathbb{Z}$ o los polinomios irreducibles de $\mathbb{F}[\mathbb{X}]$, con $\mathbb{F}$ un cuerpo, son irreducibles.

2.7 Teorema. Sea D un dominio de integridad y sea $0 \neq p \in D$ que no es unidad. las siguientes condiciones son equivalentes:

(i) p es irreducible.

(ii) Si $d|p$, entonces d es inversible o $d \sim p$.

(iii) Si $p = ab$ entonces $p \sim a$ o $p \sim b$.

2.8 Corolario. Sea D un dominio de integridad y sean $a, b \in D$ con a irreducible. Entonces si $b \sim a$, b es irreducible.

2.9 Def. Se dice que un dominio de integridad verifica la condición de cadena ascendente (C.C.A.) para sus ideales principales si toda cadena de ideales principales,

$$Da_1 \subset Da_2 \subset \cdots \subset Da_n \subset \cdots$$

es estacionaria. Es decir, existe $k \in \mathbb{N}$ tal que $Da_k = Da_{k+s}$ para todo $s \in \mathbb{N}$.

2.10 Teorema. Sea D un dominio de integridad que satisface C.C.A. para sus ideales principales. Entonces todo elemento de D se puede escribir como producto de elementos irreducibles.

3. DOMINIOS DE FACTORIZACIÓN ÚNICA (DFU)

3.1 Def. Se dice que un dominio de integridad D es un dominio de factorización única si para todo elemento no nulo $a \in D$, con a no inversible se tiene:

(i) a se factoriza como producto de irreducibles.

(ii) Si $a = p_1 \cdots p_r = q_1, \cdots q_s$ con p_i, q_i irreducibles, entonces $r = s$ y existe $\sigma \in S_r$ (el grupo de permutaciones con r elementos) tal que p_i es asociado a $q_{\sigma(i)}$ para $i = 1, 2, \ldots, r$.

Nota: Sabemos que $\mathbb{Z}$ y $\mathbb{F}[X]$ son DFU.

3.2 Def. Sea D un dominio de integridad. Se dice que un elemento $p \in D$ es primo si para todo par de elementos $a, b \in D$, si $p|ab$ entonces $p|a$ o $p|b$.

3.3 Lema. Sea D un dominio de integridad y sean $p, a_1, \ldots, a_n \in D$. Supongamos que p es primo y divide a $a_1 a_2 \cdots a_n$. Entonces existe $k \in \{1, 2, \ldots, n\}$ tal que $p|a_k$.

3.4 Teorema. En un dominio de integridad D los elementos primos son irreducibles. Es más, si D es un DFU, se tiene el recíproco.

3.5 Teorema. Sea D un dominio de integridad. Las siguientes condiciones son equivalentes:

(i) D verifica CCA y todo elemento irreducible de D es primo.

(ii) D es un DFU.

3.6 Proposición. Sea D un dominio de factorización única. Sea $a \in D$ que factoriza como producto de primos $a = p_1^{n_1} \cdots p_k^{n_k}$, con $n_i \in \mathbb{N}$. Entonces los divisores de a, salvo asociados, son de la forma $p_1^{m_1} \cdots p_k^{m_k}$, con $m_i \leq n_i$.

3.7 Def. Sea D un DFU. y sean $a_1, a_2, \ldots, a_n \in D$.

$\star$ Se define el máximo común divisor de $a_1, \ldots, a_n$ y se representa por

$$m.c.d(a_1, a_2, \ldots, a_n)$$

a cualquier $d \in D$ con las siguientes propiedades:

(i) $d|a_i$ para $i = 1, 2, \ldots, n$.

(ii) Si $r|a_i$ para $i = 1, 2, \ldots, n$, entonces $r|d$.

$\star$ Se define el mínimo común múltiplo $a_1, \ldots, a_n$ y se representa por

$$M.C.M(a_1, a_2, \ldots, a_n)$$

a cualquier $d' \in D$ con las siguientes propiedades:

(i) $a_i|d$ para $i = 1, 2, \ldots, n$.

(ii) Si $a_i|r$ para $i = 1, 2, \ldots, n$, entonces $d|r$.

$\star$ Es fácil de demostrar que el máximo común divisor y el mínimo común múltiplo, si existe, son únicos salvo asociados.

3.8 Teorema. Sea D un dominio de factorización única y sean $a_1, \ldots, a_n \in D$ no nulos ni unidades. Sean $p_1, \ldots, p_k$ elementos primos de D tales que para cada $i \in \{1, \ldots, n\}$, $a_i = p_1^{n_1^i} \cdots p_k^{n_k^i}$. Entonces:

(i) $m.c.d(a_1, a_2, \ldots, a_n)$ consiste en el producto de los primos comunes con el menor exponente.

(ii) $M.C.M(a_1, a_2, \ldots, a_n)$ consiste en el producto de los primos comunes y no comunes con el mayor exponente.

Por tanto, dados $a, b \in D$ no nulos ni unidades,

$$a\ b = m.c.d(a, b)\ M.C.M(a, b).$$

Nota: El teorema de Bezout no se tiene que verificar para DFU.

3.9 Teorema. Si D es un DFU, entonces $D[X]$ es un DFU.

4. DOMINIOS DE IDEALES PRINCIPALES (DIP)

Sea D un dominio de integridad, o más generalmente, sea D un anillo conmutativo y unitario. Sabemos entonces que dado $a \in D$ el ideal generado por a es Da. (en un anillo arbitrario R es $< a >= RaR + Ra + aR + \mathbb{Z}a$).

Nota: Durante esta sección denotaremos indistintamente al ideal generado por a como Da o $< a >$.

4.1 Def. Se dice que un dominio de integridad D es un dominio de ideales principales (DIP) si todo ideal de D es principal, es decir, si I es un ideal de D, existe $a \in I$ tal que $I = Da$.

Nota: Sabemos que $\mathbb{Z}$ y $\mathbb{F}[X]$ con $\mathbb{F}$ un cuerpo son dominios de ideales principales: Los ideales de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$ para $n \in \mathbb{N}$ y si I es un ideal de $\mathbb{F}[X]$ y $p(x)$ es un polinomio de I con grado mínimo, entonces $I =< p(x) >$.

4.2 Proposición. Todo DIP verifica CCA para sus ideales.

4.3 Proposición. En un DIP los elementos irreducibles son primos.

4.4 Teorema. Todo DIP es un DFU.

4.5 Proposición. Sea D un DIP y sean $a_1, \ldots, a_n \in D$ no nulos ni inversibles. Entonces:

(i) $d = m.c.d(a_1, \ldots, a_n)$ si y sólo si $Da_1 + Da_2 + \cdots + Da_n = Dd$.

(i) $d = M.C.M(a_1, \ldots, a_n)$ si y sólo si $Da_1 \cap Da_2 \cap \cdots \cap Da_n = Dd$.

Nota: Como corolario de (i) se obtiene el teorema de Bezout para DIP (recordamos que no era cierto para DFU).

4.6 Teorema. Sea D un DIP y sea $0 \neq p \in D$. Las siguientes condiciones son equivalentes:

(i) p es primo (que es lo mismo que irreducible).

(ii) Dp es un ideal maximal de D.

(iii) D/Dp es un cuerpo.

(iv) D/Dp es un dominio de integridad.

(v) Dp es un ideal primo de D.

4.7 Corolario. Si D es un DIP y I es un ideal no nulo de D, I es un ideal primo si y sólo si es maximal.

Nota: en un dominio de integridad D, el ideal nulo es siempre primo y no tiene que ser maximal (sólo es maximal si D es un cuerpo).

5. DOMINIOS EUCLíDEOS

Cuando trabajamos con $\mathbb{Z}$ o con $\mathbb{F}[X]$, el anillo de polinomios sobre un cuerpo $\mathbb{F}$, demostramos que verificaban el "algoritmo de la division". En esta sección vamos a estudiar dominios de integridad en los que existe, en cierta forma, un algoritmo de la división.

5.1 Def. Sea D un dominio de integridad. Se dice que D es un dominio euclídeo (DE) si existe una función $\delta : D^* \to \mathbb{N}^*$ tal que:

(i) dados $a, b \in D$ con $b \neq 0$ existe $c, r \in D$ tales que $a = cb + r$ en donde $r = 0$ o $\delta(r) < \delta(b)$.

(ii) para todo par de elementos no nulos $a, b \in D$, $\delta(a) \leq \delta(ab)$.

Nota: $\mathbb{Z}$ es un dominio euclídeo en donde δ es el valor absoluto y $\mathbb{F}[X]$, el anillo de polinomios sobre un cuerpo $\mathbb{F}$ es dominio euclídeo en donde δ es la función grado.

5.2 Teorema. Todo DE es un DIP.

5.3 Teorema. En DE se verifica el algoritmo euclídeo. Es decir,

$\star$ dados $a, b \in D$ no nulos, si $a = cb + r$, entonces $m.c.d(a, b) = m.c.d(b, r)$

Por tanto, la función Euclídea permite un método recursivo para calcular el máximo común divisor de dos elementos no nulos:

Sean a, b dos elementos no nulos de un dominio Euclídeo D. Aplicacos el algoritmo de la división a a, b

$$\begin{aligned}
a &= c_1 b + r_1 && \text{Si} \quad r_1 \neq 0, \quad \delta(r_1) < \delta(b) \\
b &= c_2 r_1 + r_2 && \text{Si} \quad r_2 \neq 0, \quad \delta(r_2) < \delta(r_1) \\
r_1 &= c_3 r_2 + r_3 && \text{Si} \quad r_3 \neq 0, \quad \delta(r_3) < \delta(r_2) \\
&\vdots \\
r_n &= c_3 r_{n+1} + r_{n+2} && \text{Si} \quad r_{n+2} \neq 0, \quad \delta(r_{n+2}) < \delta(r_{n+1})
\end{aligned}$$

Como $\delta(b) > \delta(r_1) > \cdots > \delta(r_n) > \cdots$, existe un k tal que $r_k = 0$. Para este k se tiene que $r_{k-2} = c_k r_{k-1}$ y por la propiedad $\star$

$$m.c.d(a, b) = m.c.d(b, r_1) = \cdots = m.c.d(r_{k-2}, r_{k_1}) = m.c.d(c_k r_{k-1}, r_{k_1}) = r_{k-1}.$$

6. EL ANILLO DE LOS ENTEROS DE GAUSS

En esta última sección vamos a estudiar una familia de anillos que aparecen al adjuntar a $\mathbb{Z}$ un elemento $\omega \in \mathbb{C}$ tal que $\omega^2 \in \mathbb{Z}$ (es decir, ω es solución del polinomio $X^2 - \omega^2 \in \mathbb{Z}[X]$).

6.1 Def. Sea $\omega \in \mathbb{C}$ tal que $\omega^2 \in \mathbb{Z}$ y $\omega \notin \mathbb{Z}$. Consideremos el subanillo de $\mathbb{C}$ generado por $\mathbb{Z}$ y ω, denotado por $\mathbb{Z}[\omega]$. Es claro que tienes que contener a $\mathbb{Z}$, y a $\mathbb{Z}\omega$ y a sumas de estos elementos. Es fácil ver que no contiene elementos nuevos:

$$\mathbb{Z}[\omega] = \{n + m\omega \quad | \quad n, m \in \mathbb{Z}\}$$

Nota: Dado $\xi \in \mathbb{C}$ consideremos el homomorfismo evaluación $\Phi_\xi : \mathbb{Z}[X] \to \mathbb{C}$ que a cada $p(x) \in \mathbb{Z}[X]$ le hace corresponder $p(\xi)$. Entonces $\operatorname{Im} \Phi_\xi \cong \mathbb{Z}[\xi] \cong \mathbb{Z}[X]/(\operatorname{Ker}(\Phi_\xi))$.

6.2 Lema. Sea $\omega \in \mathbb{C}$ tal que $\omega^2 \in \mathbb{Z}$ y $\omega \notin \mathbb{Z}$. Entonces:

(i) $w \notin \mathbb{Q}$.

(ii) Si $n + m\omega = n' + m'\omega \in \mathbb{Z}[\omega]$, entonces $n = n'$ y $m = m'$.

Nota: Recordamos el anillo de los enteros de Gauss que corresponde a $\mathbb{Z}[i]$ con i la raíz imaginaria ($i^2 = -1$).

6.3 Def. Sea $\omega \in \mathbb{C}$ tal que $\omega^2 \in \mathbb{Z}$ y $\omega \notin \mathbb{Z}$. Consideremos $\mathbb{Z}[\omega]$:

$\star$ Se define el conjugado de un elemento $n + m\omega \in \mathbb{Z}[\omega]$ y se representa por $(n + m\omega)^*$ como

$$(n + m\omega)^* := n - m\omega.$$

$\star$ Se define la norma de un elemento $n + m\omega \in \mathbb{Z}[\omega]$ y se representa por $N(n + m\omega)$ como

$$N(n + m\omega) := n^2 - \omega^2 m^2.$$

6.4 Proposición. Sea $\omega \in \mathbb{C}$ tal que $\omega^2 \in \mathbb{Z}$ y $\omega \notin \mathbb{Z}$. Sean $a, b \in \mathbb{Z}[\omega]$, entonces:

(i) $aa^* = a^*a = N(a) = N(a^*)$.

(ii) $(ab)^* = a^*b^*$ y $a^{**} = a$.

(iii) $N(ab) = N(a)N(b)$.

(iv) a es una unidad de $\mathbb{Z}[\omega]$ si y sólo si $N(a) = \pm 1$. Además, $a^{-1} = N(a)\ a^*$.

(v) $N(a) = 0$ si y sólo si $a = 0$.

(vi) Si $N(a)$ es un primo de $\mathbb{Z}$, entonces a es irreducible en $\mathbb{Z}[\omega]$.

6.5 Teorema. Sea $\omega \in \mathbb{C}$ tal que $\omega^2 \in \mathbb{Z}$ y $\omega \notin \mathbb{Z}$. Entonces $\mathbb{Z}[\omega]$ verifica la C.C.A para sus ideales principales. En particular todo elemento de $\mathbb{Z}[\omega]$ factoriza como producto de irreducibles.

6.6 Teorema. Sea $\omega \in \mathbb{C}$ tal que $\omega^2 \in \mathbb{Z}$ y $\omega \notin \mathbb{Z}$. Supongamos que para cada $r, s \in \mathbb{Q}$ existen $n, m \in \mathbb{Z}$ tales que

$$|(r - m) - \omega^2(s - n)| < 1$$

Entonces $\mathbb{Z}[\omega]$ es un dominio euclídeo, con función Euclídea $\delta(a) = |N(a)|$.

6.7 corolario. EL anillo de los enteros de Gauss es un dominio euclídeo.

Nota: Las unidades de $\mathbb{Z}[i]$ son $\pm 1, \pm i$.

Estudiemos ahora cuales son los elementos irreducibles de $\mathbb{Z}[i]$. Ya sabemos que dado $a = n + mi \in \mathbb{Z}[i]$, si $N(a)$ es un número primo, a es irreducible.

En primer lugar podríamos pensar que todo primo de $\mathbb{Z}$ es primo en $\mathbb{Z}[i]$, pero es falso: $5 = (2+i)(2-i)$ (esta es la factorización de 5 como producto de primos).

6.8 Proposición. Un número primo $p \in \mathbb{Z}$ es primo en $\mathbb{Z}[i]$ si y sólo si no se puede escribir como suma de dos cuadrados.

Demo: Supongamos que p se puede escribir como suma de dos cuadrados, $p = n^2 + m^2$. Entonces

$$p = (n + mi)(n - mi)$$

en donde $n + mi, n - mi$ si son primos de $\mathbb{Z}[i]$ (ya que su norma es un número primo).

Supongamos que $p = (n + mi)(n' + m'i)$, en donde $n + mi$, $n' + m'i$ no son unidades. Podemos suponer n, m son primos entre si, entonces:

$$nn' - mm' = p \qquad (*)$$
$$nm' + mn' = 0 \qquad (**)$$

veamos varios casos:

$\star$ Si $n = 0$, entonces $p = mi\ (n' + m'i) = -mm' + mn'i$, por tanto $n' = 0$ y $p = -mm'$ implica que m o m' es ± 1 (al ser p primo) y $n+mi = \pm i$ o $n'+m'i = \pm i$ es inversible.

$\star$ Si $m = 0$ llegamos al mismo resultado.

$\star$ So n, m son no nulos, entonces $nm' = -mn'$, como $m.c.d(n, m) = 1$, n divide a n', por lo que $n' = \alpha n$, Así, por $(*)$, $nm' = -n'm = -\alpha nm$, por lo que $m' = -\alpha m$. Ahora por $(**)$, $p = nn' - mm' = \alpha n^2 + \alpha m^2 = \alpha(n^2 + m^2)$ y así, como p es un primo de $\mathbb{Z}$, o $n^2 + m^2 = 1$ con lo que $n + mi$ sería inversible, o $\alpha = \pm 1$ y $p = (n + mi)(n - mi) = n^2 + m^2$, una suma de cuadrados. ■

6.9 Lema. Sea $p \in \mathbb{Z}$ un número primo tal que $p \equiv 1$ (Mod 4). Entonces la ecuación $x^2 + 1 = 0$ tiene solución en $\mathbb{Z}_p$.

Demo: En caso contrario, no habría elementos en $\mathbb{Z}_p$ tales que $x^2 = -1$ y como $\mathbb{Z}_p$ es un cuerpo para cada $r \in \mathbb{Z}_p$ existiría $s \in \mathbb{Z}_p$ con $rs = -1$ (los podré reordenar a pares), luego si multiplico todos los elementos de $\mathbb{Z}_p^*$,

$$(p-1)! \equiv (-1)^{(p-1)/2} \text{ (Mod } p)$$

y como $p \equiv 1 \pmod 4$, $(p-1)/2$ es par por lo que

$$(p-1)! \equiv 1 \pmod p$$

que contradice el teorema de Wilson $(p-1)! \equiv -1 \pmod p$. ■

6.10 Teorema. Sea $p \in \mathbb{Z}$ un número primo. Entonces p es irreducible en $\mathbb{Z}[i]$ si y sólo si $p \equiv 3 \pmod 4$.

Demo: Supongamos que p es reducible. Entonces por el teorema anterior $p = n^2 + m^2$ con $n, m \in \mathbb{N}$. Si $p = 2$, $p \equiv 2 \pmod 4$ y si p es impar, n es par y m es impar o viceversa, podemos suponer n par, por lo que

$$p \equiv n^2 + m^2 \equiv 0 + 1^1 \equiv 1 \pmod 4 \qquad \text{ó,}$$
$$p \equiv n^2 + m^2 \equiv 0 + 3^3 \equiv 1 \pmod 4$$

Supongamos ahora que p es irreducible y no es congruente con 3 módulo 4. Entonces,

⋆ p no puede ser congruente con cero módulo 4 (ya que es primo).

⋆ Si $p \equiv 2 \pmod 4$, $p = 2$ que es reducible, contradicción.

⋆ Luego $p \equiv 1 \pmod 4$. Tenemos entonces que la ecuación $x^2 + 1 \equiv 0 \pmod p$ tiene solución por lo que existe $u \in \mathbb{Z}$ tal que $u^2 + 1$ es divisible por p, pero en $\mathbb{Z}[i]$, $u^2 + 1 = (u+i)(u-i)$ y como es primo, p dividiría a $u - i$ o a $u + i$, una contradicción. ■

6.11 Teorema. Sea $z = n + mi \in \mathbb{Z}[i]$, el anillo de los enteros de Gauss. Entonces z es irreducible (y por tanto primo) si y sólo si se verifica una de las siguientes condiciones:

(i) $N(z)$ es un número primo.

(ii) $z \in \mathbb{Z}$ es un número primo con $z \equiv 3 \pmod 4$ o asociado a éste.

Demo: Por los teoremas anteriores, los elementos que verifican (i) y (ii) son irreducibles. Supongamos ahora que $z \in \mathbb{Z}[i]$ es irreducible y consideremos $N(z)$. Factorizamos $N(z)$ como producto de primos de $\mathbb{Z}$ y si p es uno de estos primos y es reducible sobre $\mathbb{Z}[i]$ lo escribimos como $p = (n + mi)(n - mi)$ producto de primos por (i),(con $n^2 + m^2 = p$) luego como z divide a $N(z)$, y es primo tiene que dividir a alguno de estos y por tanto es (salvo equivalencia) uno de estos. ■

6.12 Veamos un proceso para factorizar un número de Gauss: Consideremos $n + mi \in \mathbb{Z}[i]$.

⋆ Paso primero: calculamos la norma de z.

$$N(z) = n^2 + m^2$$

⋆ Paso segundo: factorizamos en $\mathbb{Z}$ el número entero $N(z)$.

$$N(z) = p_1^{n_1} \cdots p_k^{n_k}$$

⋆ Paso tercero: Factorizamos cada uno de los primos que aparecen.

⋆ Paso final: Como $N(z) = zz^*$, y $\mathbb{Z}[i]$ es un dominio de factorización única, al ser un dominio euclídeo, de la factorización en primos de $N(z)$ sólo nos tenemos que quedar con los que corresponden a z (que son justamente la mitad).

Nota: Si p_i está en la factorización de $N(z)$ y es primo de $\mathbb{Z}[i]$, por tanto $p_i \equiv 3$ (Mod 4), entonces debe de aparecer elevado a un número par.

7. 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).

⋆ **J. Dorronsoro y E. Hernández** , "Números, Grupos y Anillos". Addison-Wesley (1996).