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.

Proof: 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.

Proof: 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.

Proof: 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.

Proof: 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.

Proof: 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.

Proof: 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).