Universidad del Atlántico

Revista Del Programa De Matemáticas (2014) 25–39

Facultad de Ciencias Básicas

©Programa de Matemáticas

Vol. I , Nº 2, (2014)

Matrices Rectangulares Invertibles

Rectangular Invertible Matrices

German Esteban Gómez Angarita[1]

[1]*Programa de Matemáticas, Universidad del Atlántico*
gerests@gmail.com

Oswaldo Dede Mejía[2]

[2]*Programa de Matemáticas, Universidad del Atlántico*
dedemejia@gmail.com

Recibido: 02/12/2013 - Aceptado: 03/03/2014

Resumen

Sea n un entero positivo y R un anillo con elemento identidad; notamos por R^n el R-módulo izquierdo cuyos elementos son de la forma: $\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ tal que $x_i \in R$ para cada $1 \leq i \leq n$. En el presente trabajo, se estudian condiciones de invertibilidad de matrices rectangulares sobre R vía relaciones de congruencia en $\mathbb{N} = \{1, 2 \cdots\}$, estipulando que anillos tienen número de base invariante.

Palabras claves: Anillos con elemento identidad, matrices invertibles sobre un anillo, número de base invariante, congruencias.

Abstract

Let n be a positive integer and R a ring with identity element, I noticed for R^n the left R-module whose elements are of the form: $\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ such that $x_i \in R$ for each $1 \leq i \leq n$. In this paper, invertibility condition of rectangular matrices over R are studied via congruence relations in $\mathbb{N} = \{1, 2, 3 \cdots\}$ stipulating that rings have invariant basis number.

Keywords: Rings with identity element, invertible matrices over a ring, invariant basis number, congruences.

1. Introducción

Este trabajo está basado en algunas ideas tomadas de [1]. Nuestra labor consistió en analizar y detallar las demostraciones allí presentadas.

En los cursos básicos de teoría de algebra lineal, solo se estudia el concepto de invertibilidad para matrices cuadradas con entradas en un campo; sin embargo hay situaciones en las cuales se presentan matrices rectangulares ´invertibles´, esto es, matrices de tamaño $m \times n$ sobre un anillo R, digamos P para la cual existe una matriz única Q de tamaño $n \times m$ sobre R tal que $PQ = I_m$ y $QP = I_n$, donde I_m e I_n son las matrices identidad de tamaño $m \times m$ y $n \times n$ respectivamente.

Cuando toda matriz invertible en un anillo R es necesariamente cuadrada, el anillo R se dice que tiene un **N**úmero de **B**ase **I**nvariante. Muchos anillos tales como los campos o los enteros tienen esta propiedad y existen resultados que muestran que tal propiedad puede transmitirse de un anillo a otro.

En el presente trabajo se dan algunos ejemplos de anillos que no tienen número de base invariante, los cuales pueden clasificarse mediante una relación de congruencia sobre los números naturales, lo que nos permite determinar el tamaño permitido de las matrices invertibles.
Tal relación de congruencia es a su vez determinado por su tipo (w, d) , el cuál es llamado el *tipo del anillo* o el *tipo de la congruencia*.

Para este estudio utilizaremos los conceptos de congruencia en $\mathbb{N} = \{1, 2, 3, ...\}$, anillos con elemento identidad y homomorfismo de anillos.

2. Preliminares

En esta sección se estudian los anillos, los subanillos, los ideales, los módulos, las relaciones de equivalencia, etc. Tales temas pueden consultarse en: [5],[6],[7].

Sea R un conjunto no vacío, dos operaciones definidas en R, " $+$ " y " $\cdot$ ". Diremos que $(R, +, \cdot)$ es un anillo si se verifica:

R_1) $(R, +)$ es un grupo abeliano;

R_2) $(R, \cdot)$ es asociativo;

R_3) Se cumplen las leyes distributivas:
$(x + y) \cdot z = x \cdot z + y \cdot z$
$x \cdot (y + z) = x \cdot y + x \cdot z$

Si el anillo satisface:

R_4) $x \cdot y = y \cdot x$ para todo $x, y \in R$ entonces R es un anillo conmutativo; además si existe $1 \in R$ tal que $\forall x \in R\ x \cdot 1 = 1 \cdot x = x$, diremos que R es un anillo con elemento identidad. Escribimos simplemente xy en vez de $x \cdot y$ y al módulo de la suma lo notaremos 0.

En R_1) cuando decimos que $(R, +)$ es un grupo abeliano significa:

(i) En el conjunto R está definida la operación binaria: $(x, y) \mapsto x + y$;

(ii) La operación es asociativa: $(x + y) + z = x + (y + z)$, para todos los $x, y, z \in R$;

(iii) R posee el elemento neutro (unidad) 0: $0 + x = x + 0 = x$ para todo $x \in R$;

(iv) Para cada elemento $x \in R$, existe el inverso $-x$: $x + (-x) = (-x) + x = 0$;

(v) R es conmutativo: $x + y = y + x$ para todos los $x, y \in R$.

Sea $\{0\} \neq R$ un anillo y $\emptyset \neq S \subseteq R$. Diremos que S es un subanillo de R si se verifica:

(i) $\forall x, \forall y\ \ x - y \in S$;

(ii) $\forall x, \forall y\ \ x - y \in S$

Sea $R \neq \{0\}$ un anillo. Para $0 \neq a \in R$ diremos que a es un divisor de cero si existe $b \in R$, $b \neq 0$ tal que $ab = ba = 0$.
Si R es un anillo conmutativo sin divisores de cero y con elemento identidad diremos que R es un dominio entero.

Todo campo es un dominio entero.

Sea $\psi : R \to S$ una función, R y S anillos. Diremos que ψ es un homomorfismo de anillos si se satisface:

i) $\psi(x + y) = \psi(x) + \psi(y)$;

ii) $\psi(xy) = \psi(x)\psi(y)$

para todo $x, y \in R$.

Sea $\psi : R \to S$ un homomorfismo de anillos, entonces:

1) $\psi(0_R) = 0_S$;

2) $\psi(-x) = -\psi(x)$;

3) $\psi(nx) = n\psi(x)$ para todo $n \in \mathbb{Z}$ y todo $x \in R$;

4) Si R y S son dominios enteros entonces o ψ es una función constante cero o $\psi(1_R) = 1_S$.

donde $0_R, 1_R$ y $0_S, 1_S$ son los módulos de $+$ y $\cdot$ para R y S respectivamente.

$\psi : R \to S$ es un isomorfismo de anillos si cumple las siguientes condiciones:

i) ψ es biyectiva ;

ii) ψ es un homomorfismo de anillos

Si los anillos R y S son isomorfos lo denotaremos como sigue: $R \approx S$.

$\psi : R \to S$ es un isomorfismo de anillos si y solamente si $\psi : R \to S$ es un homomorfismo de anillos y $\psi^{-1} : S \to R$ es un homomorfismo de anillos. **Demostración**

($\Rightarrow$) Por ser ψ biyectiva tenemos que $\psi(x) = y \Leftrightarrow \psi^{-1}(y) = x$.
Sean $y, \widehat{y} \in S$, dado que ψ es biyectiva entonces existen $x, \widehat{x}$ tal que $\psi(x) = y$, $\psi(\widehat{x}) = \widehat{y}$. Entonces $\psi^{-1}(y) = x$ y $\psi^{-1}(\widehat{y}) = \widehat{x}$. Dado que ψ es un homomorfismo de anillos entonces:

i) $\psi(x + \widehat{x}) = \psi(x) + \psi(\widehat{x}) = y + \widehat{y}$;

ii) $\psi(x\widehat{x}) = \psi(x)\psi(\widehat{x}) = y\widehat{y}$

Por i) tenemos que $\psi^{-1}(y + \widehat{y}) = x + \widehat{x} = \psi^{-1}(y) + \psi^{-1}(\widehat{y})$ y por ii) tenemos que $\psi^{-1}(y\widehat{y}) = x\widehat{x} = \psi^{-1}(y)\psi^{-1}(\widehat{y})$. Por tanto ψ^{-1} es un homomorfismo.

($\Leftarrow$) Dado que existe ψ^{-1} entonces ψ es biyectiva y además como $\psi : R \to S$ es un homomorfismo de anillos entonces por definición ψ es un isomorfismo de anillos. ■

Una matriz A con n filas y n columnas se denomina matriz cuadrada de orden n.

Si A es una matriz cuadrada y si se puede encontrar una matriz B del mismo tamaño tal que $AB = BA = I$ entonces se dice que A es *invertible* y B se denomina una inversa de A.

Si B y C son, ambas, inversas de la matriz A, entonces $B = C$.

Si A y B son matrices invertibles del mismo tamaño, entonces

a) AB es invertible,

b) $(AB)^{-1} = B^{-1}A^{-1}$

Si A es una matriz cuadrada, entonces las potencias enteras no negativas de A se definen como $A^0 = I \quad A^n = AA \underbrace{\cdots}_{n factores} A \ (n > 0)$. Además, si A es invertible, entonces las potencias enteras negativas de A se definen como $A^{-n} = (A^{-1})^n = A^{-1}A^{-1} \underbrace{\cdots}_{n factores} A^{-1}$.

Si A es una matriz cuadrada y r y s son enteros, entonces $A^r A^s = A^{r+s}$ y $(A^r)^s = A^{rs}$.

Si A es una matriz cuadrada e invertible, entonces

a) A^{-1} es invertible y $(A^{-1})^{-1} = A$.

b) A^n es invertible y $(A^n)^{-1} = (A^{-1})^n$ para $n = 0, 1, 2 \cdots$

c) Para cualquier $k \in \mathbb{R}$ diferente de cero, la matriz kA es invertible y $(kA)^{-1} = \frac{1}{k}A^{-1}$.

Si A es una matriz invertible, entonces A^T también es invertible y $(A^T)^{-1} = (A^{-1})^T$.

Sea R un anillo, I un subanillo de R.

i) Si para todo $i \in I$ y para todo $r \in R$ se verifica que $ri \in I$, diremos que I es un ideal izquierdo de R ;

ii) Si para todo $i \in I$ y para todo $r \in R$ se verifica que $ir \in I$, diremos que I es un ideal derecho de R.

Si se cumple i) y ii) diremos que I es un ideal bilateral de R o simplemente un ideal de R.

Si R es un anillo, $aR = \{ar \mid r \in R\}$ y $Ra = \{ra \mid r \in R\}$ son ideales derecho e izquierdo de R respectivamente.

Si I y K son ideales entonces definimos $I + K = \{i + k \mid i \in I, k \in K\}$ e

$$IK = \{\sum_{i=1}^{m} a_i b_i \mid a_i \in I, b_i \in K, m \in \mathbb{N}\}$$

.

Si I y K son ideales de un anillo R, entonces:

i) $I \cap K$ es un ideal de R ;

i) $I + K$ es un ideal de R ;

i) IK es un ideal de R

Sea R un anillo e I un ideal de R. En $R/I = \{x + I \mid x \in R\}$ las operaciones $+$ y $\cdot$ se definen: $+ : R/I \times R/I \to R/I$, definido por $(x + I, y + I) \mapsto (x + I) + (y + I) = (x + y) + I$ y $\cdot : R/I \times R/I \to R/I$, definido por $(x + I, y + I) \mapsto (x + I) \cdot (y + I) = (x \cdot y) + I$

Sea R un anillo e I un ideal de R. Si $R/I = \{x + I \mid x \in R\}$ entonces:

i) R/I es un anillo, llamado anillo cociente de R por I ;

ii) Si 1 es el elemento identidad de R entonces $1 + I$ es el elemento identidad de R/I ;

iii) Si R es conmutativo entonces R/I es conmutativo.

Cada anillo con elemento identidad posee al menos un ideal maximal.

Sea R un anillo conmutativo con elemento identidad. Entonces M es un ideal maximal de R si y sólo si R/M es un campo.

Si R_1, R_2 son anillos con elemento identidad, $(R_1, +, \cdot)$, $(R_2, +', \cdot')$, $D = R_1 \times R_2$. En D se define para $x \in R_1, y \in R_2, u \in R_1, v \in R_2$; $(x, y) \oplus (u, v) = (x + u, y +' v)$ y $(x, y) \odot (u, v) = (x \cdot u, y \cdot' v)$. Con estas operaciones D es un anillo con elemento identidad.

Sea R un anillo con identidad y sea V un grupo abeliano escrito aditivamente. Si la aplicación $\cdot : R \times V \longrightarrow V$, definida por $\cdot(x, v) = x \cdot v := xv$ satisface las siguientes propiedades:

(M_1) $x(u + v) = xu + xv$, para todo $x \in R, u, v \in V$;

(M_2) $(x + y)v = xv + yv$, para todo $x, y \in R$, $v \in V$;

(M_3) $(xy)v = x(yv)$, para todo $x, y \in R, v \in V$;

(M_4) $1v = v$, para todo $v \in V$.

Entonces V se dice un R-módulo a izquierda o un R-módulo izquierdo. Análogamente se define R-módulo a derecha.
A menos que explícitamente se mencione lo contrario, el término módulo significará módulo izquierdo.

Módulos sobre un campo F y espacio vectoriales sobre F son lo mismo.

Un subconjunto $S = \{s_1, s_2, \ldots, s_n\}$ de un R-módulo, se dice **linealmente independiente(L.I)** si la única combinación lineal nula con los elementos de S es a través de escalares nulos de R. Más exactamente, S es linealmente independientes si para cualesquiera escalares $a_1, \cdots, a_n \in R$ se cumple que $\sum_{i=1}^{n} a_i s_i = 0 \Rightarrow a_i = 0,\ 1 \leq i \leq n$.

Nota. Por definición asumimos que el conjunto vacío es **L.I**. Un subconjunto cualquiera S de V es **L.I** si cada subconjunto finito de S es **L.I**. S es linealmente dependiente (**L.D**) si no es **L.I**.

Si $S = \{s_1, s_2, \ldots, s_n\}$ es un subconjunto de un R- módulo V, diremos que S genera a V, si para todo $v \in V$ existen $c_1, c_2, \ldots, c_n \in R$ tales que

$$v = \sum_{i=1}^{n} c_i s_i$$

lo denotaremos por $\langle S \rangle = V$.

Un subconjunto no vacío S de un R- módulo V, es una base para V si se cumplen las siguientes condiciones:

(a) $< S >= V$;

(b) S es **L.I**.

Un R-módulo es *libre* si posee al menos una base.

La relación binaria $\sim$ en X se llama *relación de equivalencia*, si para toda $x, x', x'' \in X$ se cumplen las condiciones:

(i) $x \sim x$ (*reflexividad*);

(ii) $x \sim x' \Rightarrow x' \sim x$ (*simetría*);

(iii) $x \sim x' \wedge\ x' \sim x'' \Rightarrow x \sim x''$ (*transitividad*).

La escritura $a \nsim b$ expresa la negación de la equivalencia entre los elementos $a, b \in X$.

El subconjunto $\overline{x} = \{x' \in X \mid x' \sim x\} \subseteq X$ de todos los elementos equivalentes a un x dado, se denomina *clase de equivalencia* contenedora de x.

Dada una familia $\{B_i\}_{i \in I}$ no vacía de subconjuntos de X, $\{B_i\}_{i \in I}$ es una *partición* de X si

P_1 : $\bigcup_{i \in I} B_i = X$

P_2 : Para cualesquiera $B_i,\ B_j$, o bien $B_i = B_j$ o bien $B_i \bigcap B_j = \emptyset$.

Sea $\sim$ una relación de equivalencia en un conjunto X y para todo $x \in X$
sea $\overline{x} = \{x' \in X \mid x' \sim x\}$. Entonces la familia de conjuntos $\{\overline{x} \mid x \in X\}$ es una partición de X. El conjunto de clases de equivalencia se denota por $X/\sim$, que es llamado el *conjunto cociente*.

3. Anillos con número de base invariante

Normalmente se habla de matrices invertibles cuando son cuadradas. Sin embargo hay situaciones en las que se producen matrices rectangulares *invertibles* .

Durante todo el trabajo usaremos anillos R con elemento identidad y
$\mathbb{N} = \{1, 2, \cdots\}$.

Decimos que una matriz P de tamaño $m \times n$ con entradas en R, es invertible si existe una matriz Q de tamaño $n \times m$ con entradas en R tal que $PQ = I_m$ y $QP = I_n$, donde I_m e I_n son las matrices identidad de tamaños $m \times m$ y $n \times n$ respectivamente.

Si la matriz Q de $n \times m$ existe entonces es única. **Demostración**

Sean S y Q matrices de tamaño $n \times m$ tal que $PS = I_m$ y $SP = I_n$ y $PQ = I_m$ y $QP = I_n$

$S(PQ) = (SP)Q = I_nQ = Q$ y $S(PQ) = SI_m = S$. Entonces $Q = S$. ■

Un anillo R se dice que tiene un **N**úmero de **B**ase **I**nvariante si y solamente si toda matriz invertible con entradas en R es cuadrada.
Si un anillo tiene **N**úmero de **B**ase **I**nvariante lo denotaremos **NBI**. Es decir, R tiene **NBI** $\Leftrightarrow (\forall P)(P$ es invertible $\Rightarrow P$ es cuadrada).

Algunos anillos conocidos como los enteros y los campos gozan de esta propiedad. Algunos resultados fundamentales muestran que la propiedad de tener un número de base invariante puede transmitirse de un anillo a otro (mediante homomorfismo de anillos).

Sea n un entero, $n \geq 1$ y R un anillo.
Escribimos $R^n = \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} : x_i \in R, i = 1, \cdots, n \right\}$.

El *rango* de un R-módulo es la cardinalidad de la base.

R^n es un R-módulo libre de rango n.

Si F es un campo, P es una matriz de $m \times n$ sobre F y $T: F^n \longrightarrow F^m$, definida por $T(x) = Px$; entonces T es una transformación lineal, es decir, para todo $x, y \in F^n$ y *paratodor* $\in R$

i) $T(x + y) = T(x) + T(y)$

ii) $T(rx) = rT(x), r \in F$

Demostración

Sean $x, y \in F^n, r \in F$. Entonces
$T(x + y) = P(x + y) = Px + Py = T(x) + T(y)$
y
$T(rx) = P(rx) = r(Px) = rT(x)$
Por tanto T es una transformación lineal.

Si F es un campo, P es una matriz invertible de tamaño $m \times n$ sobre F y $T: F^n \longrightarrow F^m$ es una transformación lineal entonces los vectores $T(e_1) = Pe_1, \cdots, T(e_n) = Pe_n$ forman una base para F^m. **Demostración**

Dado que P es una matriz invertible de tamaño $m \times n$ entonces existe Q de tamaño $n \times m$ tal que $PQ = I_m$ y $QP = I_n$.
Veamos que $T(e_1) = Pe_1, \cdots, T(e_n) = Pe_n$ son linealmente independientes. Sean $c_1, \cdots, c_n \in F$, tales que
$c_1(Pe_1) + c_2(Pe_2) + \cdots + c_n(Pe_n) = 0 \Rightarrow$
$P(c_1e_1) + P(c_2e_2) + \cdots + P(c_ne_n) = 0 \Rightarrow$
$P(c_1e_1 + c_2e_2 + \cdots + c_ne_n) = 0 \Rightarrow$
$QP(c_1e_1 + c_2e_2 + \cdots + c_ne_n) = 0 \Rightarrow$
$I_n(c_1e_1 + c_2e_2 + \cdots + c_ne_n) = 0 \Rightarrow$
$c_1e_1 + c_2e_2 + \cdots + c_ne_n = 0 \Rightarrow c_1 = c_2 = \cdots = c_n = 0$, pués $\{e_1, \cdots, e_n\}$ forma una base para F^n.

Veamos que $T: F^n \longrightarrow F^m$ es sobreyectiva. Sea $w \in F^m$, definamos $x = Qw$ entonces $x \in F^n$ y $T(x) = Px = P(Qw) = (PQ)w = I_mw = w$. Por tanto T es sobreyectiva.

Veamos que $T(e_1) = Pe_1, \cdots, T(e_n) = Pe_n$ genera a F^m. Sea $s \in F^m$, como T es sobreyectiva existe $q \in F^n$ tal que $T(q) = s$ pero $q = \sum_{i=1}^n c_ie_i$ entonces $s = T(\sum_{i=1}^n c_ie_i) = \sum_{i=1}^n c_iT(e_i) = \sum_{i=1}^n c_iPe_i$ ■.

Si F es un campo entonces F tiene **NBI**.

Demostración

Sea P una matriz invertible de tamaño $m \times n$ sobre F. Por la proposición anterior se tiene que $T(e_1) = Pe_1, \cdots, T(e_n) = Pe_n$ forman una base para F^m con n elementos. Dado que F^m es un espacio vectorial entonces el número de elementos de una base es la dimensión que sabemos que es única entonces $n = m$. Por tanto toda matriz P invertible sobre F es cuadrada, por tanto F tiene **NBI** ■.

Supongamos que $f: R \longrightarrow S$ es un homomorfismo de anillos y P es una matriz invertible con entradas en R. Supongamos que P tiene inversa Q, entonces $f(P)$ tiene inversa la cuál es $f(Q)$. **Demostración**

$P = [p_{ij}]$ y $Q = \left[q_{jk}\right]$

$PQ = \left[\sum p_{ij}q_{jk}\right] = [\delta_{ik}]$, donde $\delta_{ik} = \begin{cases} 1 & \text{si } i = k \\ 0 & \text{si } i \neq k \end{cases}$

$$\begin{aligned} f(PQ) = f(\left[\sum p_{ij}q_{jk}\right]) &= \left[\sum f(p_{ij}q_{jk})\right] \\ &= \left[\sum f(p_{ij})f(q_{jk})\right] \\ &= f(P)f(Q) \end{aligned}$$

Es decir, $f(PQ) = f(P)f(Q)$, pero $PQ = I_R$, entonces $f(P)f(Q) = f(PQ) = f(I_R) = I_S$, entonces $f(P)f(Q) = I_S$, análogamente $f(Q)f(P) = I_S$, entonces $f(P)$ tiene inversa $f(Q)$. ■

Sea $f: R \longrightarrow S$ es un homomorfismo de anillos. Si S tiene **NBI** entonces R tiene **NBI**.

Demostración por contrarecíproca

Supongamos que R no tiene **NBI** entonces existe una matriz invertible P de tamaño $m \times n$ y $m \neq n$ con entradas en R. Entonces existe Q de tamaño $n \times m$ tal que $PQ = I_m$ y $QP = I_n$. Tenemos que:
$f(I_m) = f(PQ) = f(P)f(Q)$ y $f(I_n) = f(QP) = f(Q)f(P)$
Es decir $f(P)$ es una matriz invertible de $m \times n$ y $m \neq n$, es decir no cuadrada, esto significa que S no tiene **NBI** ■.

Supongamos que R es conmutativo entonces existe un homomorfismo $\phi: R \longrightarrow F$ para algún campo F. **Demostración**

Dado que R es un anillo conmutativo con elemento identidad entonces tiene un ideal máximal M y entonces $F = R/M$ es un campo. Ahora $\phi : R \to F$, la definimos $r \mapsto r + M$ y además definimos la $+$ y $\cdot$ en $F = R/M$.

i) $(r + M) + (r' + M) = (r + r') + M$

ii) $(r + M) \cdot (r' + M) = (r \cdot r') + M$

Veamos que ϕ es un homomorfismo de anillos.

$$\begin{aligned} \phi(r + r') \overset{\text{def}}{=} (r + r') + M &= (r + M) + (r' + M) \\ &= \phi(r) + \phi(r') \end{aligned}$$

Es decir $\phi(r + r') = \phi(r) + \phi(r')$.

$$\begin{aligned} \phi(r \cdot r') \overset{\text{def}}{=} (r \cdot r') + M &= (r + M) \cdot (r' + M) \\ &= \phi(r) \cdot \phi(r') \end{aligned}$$

Es decir, $\phi(r \cdot r') = \phi(r) \cdot \phi(r')$ ■.

Todo anillo conmutativo con elemento identidad tiene **NBI**. **Demostración**

Dado que existe un homomorfismo $\phi : R \to F$ para algún campo F y F tiene **NBI** entonces por proposición R tiene **NBI**. ■

El **ejemplo** de un anillo sin **NBI** es provisto por el cono $C(R)$ de un anillo R.
Los elementos de $C(R)$ son las matrices infinitas sobre R, con filas y columnas indexadas por los números naturales, cada fila y columna tiene únicamente un número finito de entradas distintas de cero.

Los elementos

$$\beta = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0\cdots \\ 0 & 0 & 1 & 0 & 0 & 0\cdots \\ 0 & 0 & 0 & 0 & 1 & 0\cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix} \quad y \quad \gamma = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0\cdots \\ 0 & 0 & 0 & 1 & 0 & 0\cdots \\ 0 & 0 & 0 & 0 & 0 & 1\cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}$$

de $C(R)$ da una matriz $\lambda = \begin{pmatrix} \beta \\ \gamma \end{pmatrix}$ de 2×1, con la matriz inversa transpuesta $\lambda' = \begin{pmatrix} \beta^t & \gamma^t \end{pmatrix}$.

En efecto,

$$\beta^t = \begin{pmatrix} 1 & 0 & 0\cdots \\ 0 & 0 & 0\cdots \\ 0 & 1 & 0\cdots \\ 0 & 0 & 0\cdots \\ 0 & 0 & 1\cdots \\ 0 & 0 & 0\cdots \\ \vdots & \vdots & \vdots \end{pmatrix} \quad y \quad \gamma^t = \begin{pmatrix} 0 & 0 & 0\cdots \\ 1 & 0 & 0\cdots \\ 0 & 0 & 0\cdots \\ 0 & 1 & 0\cdots \\ 0 & 0 & 0\cdots \\ 0 & 0 & 1\cdots \\ \vdots & \vdots & \vdots \end{pmatrix}$$

$$\beta\beta^t = \begin{pmatrix} 1 & 0 & 0\cdots \\ 0 & 1 & 0\cdots \\ 0 & 0 & 1\cdots \\ \vdots & \vdots & \vdots \end{pmatrix} =$$

$$I_{C(R)} \quad y \quad \gamma\gamma^t = \begin{pmatrix} 1 & 0 & 0\cdots \\ 0 & 1 & 0\cdots \\ 0 & 0 & 1\cdots \\ \vdots & \vdots & \vdots \end{pmatrix} = I_{C(R)}$$

$$\beta^t\beta = \begin{pmatrix} 1 & 0 & 0\cdots \\ 0 & 0 & 0\cdots \\ 0 & 0 & 1\cdots \\ \vdots & \vdots & \vdots \end{pmatrix} \quad y \quad \gamma^t\gamma = \begin{pmatrix} 0 & 0 & 0\cdots \\ 0 & 1 & 0\cdots \\ 0 & 0 & 0\cdots \\ \vdots & \vdots & \vdots \end{pmatrix}$$

Además $\beta^t\beta + \gamma^t\gamma = I_{C(R)}$

$$\beta\gamma^t = \begin{pmatrix} 0 & 0 & 0\cdots \\ 0 & 0 & 0\cdots \\ 0 & 0 & 0\cdots \\ \vdots & \vdots & \vdots \end{pmatrix} =$$

$$0_{C(R)} \quad y \quad \gamma\beta^t = \begin{pmatrix} 0 & 0 & 0\cdots \\ 0 & 0 & 0\cdots \\ 0 & 0 & 0\cdots \\ \vdots & \vdots & \vdots \end{pmatrix} = 0_{C(R)}$$

Entonces,

$$\lambda\lambda' = \begin{pmatrix} \beta \\ \gamma \end{pmatrix}_{2\times 1} \begin{pmatrix} \beta^t & \gamma^t \end{pmatrix}_{1\times 2} = \begin{pmatrix} \beta\beta^t & \beta\gamma^t \\ \gamma\beta^t & \gamma\gamma^t \end{pmatrix}_{2\times 2} = \begin{pmatrix} I_{C(R)} & 0_{C(R)} \\ 0_{C(R)} & I_{C(R)} \end{pmatrix}_{2\times 2} = E_2 \text{ y}$$

$$\lambda'\lambda = \begin{pmatrix} \beta^t & \gamma^t \end{pmatrix}_{1\times 2} \begin{pmatrix} \beta \\ \gamma \end{pmatrix}_{2\times 1} = \left(\beta^t\beta + \gamma^t\gamma\right)_{1\times 1} = \left(I_{C(R)}\right)_{1\times 1} = E_1$$

Por tanto, $C(R)$ no tiene **NBI**.

4. Congruencias en $\mathbb{N}$ y matrices rectangulares invertibles

Dados un anillo R y $a, b \in \mathbb{N}$, decimos que $a \sim_R b$ si y sólo si existe una matriz P invertible de tamaño $a \times b$ sobre R.

$\sim_R$ es una *congruencia* en $\mathbb{N}$, es decir, que $\sim_R$ es una relación de equivalencia y satisface la propiedad *aditiva* en $\mathbb{N}$, esto es:
Si $a \sim_R b \wedge c \sim_R d \Rightarrow a + c \sim_R b + d$. **Demostración**

(i) $\sim_R$ es reflexiva. En efecto, $a \sim_R a$, ya que existe una matriz $P = I_{a\times a}$ sobre R que es invertible.

$$P = \begin{pmatrix} 1_R & 0 & \cdots & 0 \\ 0 & 1_R & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1_R \end{pmatrix}_{a\times a}$$

(ii) Supongamos que $a \sim_R b$, entonces existe una matriz P invertible en R tal que P es de tamaño $a \times b$. Entonces por definición existe una matriz Q de tamaño $b \times a$ tal que $PQ = I_{a\times a}$ y $QP = I_{b\times b}$. Entonces Q es invertible y Q es de tamaño $b \times a$, entonces $b \sim_R a$. Por tanto $\sim_R$ es simétrica.

(iii) Supongamos que $a \sim_R b \wedge b \sim_R c$ entonces existe una matriz P de tamaño $a \times b$, invertible y existe Q de tamaño $b \times c$, invertible. Entonces existen W de tamaño $b \times a$ tal que $PW = I_{a\times a}$ y $WP = I_{b\times b}$ y F de tamaño $c \times b$ tal que $QF = I_{b\times b}$ y $FQ = I_{c\times c}$.
Entonces PQ es una matriz de tamaño $a \times c$, veamos que PQ es invertible.

$$\begin{aligned} PQ(FW) &= P(QF)W \\ &= P(I_{b\times b})W \\ &= (PI_{b\times b})W \\ &= PW = I_{a\times a} \end{aligned}$$

$$\begin{aligned} (FW)PQ &= F(WP)Q \\ &= F(I_{b\times b})Q \\ &= F(I_{b\times b}Q) \\ &= FQ \\ &= I_{c\times c} \end{aligned}$$

Por tanto $(PQ)(FW) = I_{a\times a}$ y $(FW)(PQ) = I_{c\times c}$. Entonces $a \sim_R c$. Así, $\sim_R$ es transitiva. Por lo tanto $\sim_R$ es una relación de equivalencia.

Veamos que $\sim_R$ satisface la propiedad *aditiva*.
Supongamos que $a \sim_R b \wedge c \sim_R d$, veamos que $a + c \sim_R b + d$.
Es decir, existe una matriz $\widehat{P}$ invertible de tamaño $a \times b$ sobre R y existe una matriz $\widehat{Q}$ invertible de tamaño $c \times d$ sobre R.

$$H = \begin{pmatrix} \widehat{P} & O \\ O & \widehat{Q} \end{pmatrix}_{(a+c)\times(b+d)}.$$

Esta matriz H es invertible. En efecto, definamos $G = \begin{pmatrix} \widehat{W} & O \\ O & \widehat{F} \end{pmatrix}$

$$HG = \begin{pmatrix} \widehat{P} & O \\ O & \widehat{Q} \end{pmatrix}\begin{pmatrix} \widehat{W} & O \\ O & \widehat{F} \end{pmatrix} = \begin{pmatrix} \widehat{P}\widehat{W} & O \\ O & \widehat{Q}\widehat{F} \end{pmatrix} = \begin{pmatrix} I_{a\times a} & O \\ O & I_{b\times b} \end{pmatrix}_{(a+b)\times(a+b)}$$

$$GH = \begin{pmatrix} \widehat{W} & O \\ O & \widehat{F} \end{pmatrix}\begin{pmatrix} \widehat{P} & O \\ O & \widehat{Q} \end{pmatrix} = \begin{pmatrix} \widehat{W}\widehat{P} & O \\ O & \widehat{F}\widehat{Q} \end{pmatrix} = \begin{pmatrix} I_{b\times b} & O \\ O & I_{c\times c} \end{pmatrix}_{(b+c)\times(b+c)}$$

Así, $a + c \sim_R b + d$. Por tanto $\sim_R$ es una congruencia en $\mathbb{N}$ ■.

Observación.
Si R tiene **NBI**, las únicas matrices invertibles son las cuadradas, entonces $a \sim_R b \Leftrightarrow a = b$.
Es decir, si R tiene **NBI** la relación $\sim_R$ es simplemente la igualdad $(=)$.

Supongamos que $\sim$ es una congruencia en $\mathbb{N}$. Entonces podemos extender $\sim$ a una congruencia $\equiv$ en $\mathbb{Z}$ diciendo que $a \equiv b$ si y sólo si existe un número natural x tal que $a + x \sim b + x$.
Demostración

Veamos que $\equiv$ es una congruencia en $\mathbb{Z}$.

(i) $\equiv$ es reflexiva. En efecto,
Si $a > 0$, $a \equiv a$ pués $\sim$ es reflexiva en $\mathbb{N}$.
Si $a \leq 0$, basta tomar $x > -a$. Entonces $a + x \sim a + x$, pués $\sim$ es reflexiva en $\mathbb{N}$. Por tanto $a \equiv a$.

(ii) $\equiv$ es simétrica. En efecto,
supongamos que $a \equiv b$, entonces existe $x \in \mathbb{N}$ tal que $a + x \sim b + x$, como $\sim$ es simétrica en $\mathbb{N}$ entonces $b + x \sim a + x$ entonces $b \equiv a$.

(iii) $\equiv$ es transitiva. En efecto,
supongamos que $a \equiv b \wedge b \equiv c$ entonces existen $x, z \in \mathbb{N}$ tal que $a + x \sim b + x$ y $b + z \sim c + z$ y como $\sim$ es una congruencia en $\mathbb{N}$, entonces tenemos que $(a + x) + (b + z) \sim (b + x) + (c + z)$ entonces $a + (x + b + z) \sim c + (x + b + z)$, entonces $a \equiv c$.

Por tanto $\equiv$ es una relación de equivalencia.

Ahora, veamos que $\equiv$ es una congruencia en $\mathbb{Z}$.
Supongamos que $a \equiv b \wedge c \equiv d$ entonces existen $x, z \in \mathbb{N}$ tal que $a + x \sim b + x$ y $c + z \sim d + z$, como $\sim$ es una congruencia en $\mathbb{N}$, tenemos que $(a + x) + (c + z) \sim (b + x) + (d + z)$, entonces $(a + c) + (x + z) \sim (b + d) + (x + z)$. Entonces $a + c \equiv b + d$.

Para evitar confusión, siempre usaremos $\sim$ para la congruencia en $\mathbb{N}$ y $\equiv$ para la congruencia en $\mathbb{Z}$. ■

Sea $\sim$ una relación de congruencia en $\mathbb{N}$, que no sea la igualdad, y $\equiv$ la relación de congruencia en $\mathbb{Z}$, determinada por ampliación de $\sim$; el menor número natural d tal que $d + x \sim x$ para algún $x \in \mathbb{N}$ se denomina el *módulo de* $\equiv$.
La existencia del d se justifica por lo siguiente:
Dada $\sim$ una relación de congruencia en $\mathbb{N}$, tomamos la relación $\equiv$ en $\mathbb{Z}$ extendida desde $\mathbb{N}$: dados $a, b \in \mathbb{Z}$, $a \equiv b$ si existe $x \in \mathbb{N}$ tal que $a + x \sim b + x$.
Tomemos la clase $[0]$ en $\mathbb{Z}$, esto es, $[0] = \{z \in \mathbb{Z} \mid z + x \sim x$, para algún $x \in \mathbb{N}\}$. Supongamos que existe $z \in [0]$, $z \in \mathbb{Z}$ y $z \neq 0$. Si $z < 0$ entonces $z + x \sim x$, para algún $x \in \mathbb{N}$. Dado que $\sim$ es una congruencia en $\mathbb{N}$ y $-z > 0$ entonces $x = z + x + (-z) \sim x + (-z)$, entonces $x \sim x + (-z)$ y por tanto $-z \in [0]$.
Tomemos $S = \{m \in \mathbb{N} \mid m + x \sim x$, para algún $x \in \mathbb{N}\} \neq \emptyset$ y $S \subseteq \mathbb{N}$. Por el principio de buena ordenación, existe d tal que $d = minS$. Así, d es el mínimo en $\mathbb{N}$ de los números $y \in \mathbb{N}$ tal que $y + x \sim x$ para algún $x \in \mathbb{N}$. En particular, existe $x \in \mathbb{N}$ tal que $d + x \sim x$ y para todo $y \in \mathbb{N}$ con $y + x \sim x$, para algún $x \in \mathbb{N}$, $d \leq y$.

Si $\equiv$ es una congruencia en $\mathbb{Z}$, definimos para $n, m \in \mathbb{N} \subseteq \mathbb{Z}$, $m \approx n \Leftrightarrow m \equiv n$. Entonces $\approx$ es una congruencia en $\mathbb{N}$, es decir restringiendo $\equiv$ a $\mathbb{N}$. **Demostración**

a) $n \approx n$ pués $n \equiv n$;

b) $n \approx m \Rightarrow n \equiv m \Rightarrow m \equiv n \Rightarrow m \approx n$;

c) Si $n \approx m \ \wedge \ m \approx s \Rightarrow n \equiv m \ \wedge \ m \equiv s \Rightarrow n \equiv s \Rightarrow n \approx s$;

d) Si $n \approx m \ \wedge \ l \approx s \Rightarrow n \equiv m \ \wedge \ l \equiv s \Rightarrow n + l \equiv m + s \Rightarrow n + l \approx m + s$.

Por tanto $\approx$ es una congruencia en $\mathbb{N}$. ■

Si $\equiv$ es la congruencia ordinaria en $\mathbb{Z}$, esto es: $a \equiv b \ (mod \ d)$ si existe $k \in \mathbb{Z}$ tal que $a = b + (k-1)d$. Restringiendo $\equiv$ en $\mathbb{N}$, tenemos que para $a, b \in \mathbb{N}$, $a \equiv b \ (mod \ d)$ si existe $k \in \mathbb{N}$ tal que $a = b + (k-1)d$.
Por tanto, para tal congruencia en $\mathbb{N}$ sus clases de equivalencia son de la forma:

$\{e + (k-1)d \mid k \in \mathbb{N}\} = \{e, e+d, e+2d, e+3d, \cdots\}$, donde $e = 1, \cdots, d$.

En efecto, dado que $a \sim b$ en $\mathbb{N}$ si y sólo si $a \equiv b \ (mod \ d)$ en $\mathbb{N}$. Entonces,

$$\begin{aligned} \{x \mid x \sim e\} &= \{x \mid x \equiv e \ (mod \ d)\} \\ &= \{x \mid x = e + (k-1)d, \ k \in \mathbb{N}\} \\ &= \{e + (k-1)d \mid k \in \mathbb{N}\} \end{aligned}$$

donde $e = 1, \cdots, d$.

$w = min\{x \in \mathbb{N} \mid x \sim x + d\}$. La existencia de w se justifica por lo siguiente:
Si $S = \{x \in \mathbb{N} \mid x \sim x + d\} \subseteq \mathbb{N}$, por definición de d, dado que $d \in [0]$ entonces existe $x \in \mathbb{N}$ tal que $x + d \sim x$, entonces $S \neq \emptyset$, por el principio de buena ordenación, existe w tal que $w = minS$.

Para d y w definido anteriormente, el par (w, d) es llamado el tipo de la congruencia o el tipo del anillo.

Sea $\sim$ una relación de congruencia en $\mathbb{N}$ que no es la igualdad. Entonces existen números naturales w y d tal que el conjunto de clases de equivalencia bajo $\sim$ comprende $w - 1$ clases $\{1\}, \{2\}, \cdots, \{w-1\}$. Junto con d clases infinitas $\{e, e+d, e+2d, \cdots\}$, $e = w, w+1, \cdots, w+d-1$.

Recíprocamente, cualquier partición de $\mathbb{N}$ da una relación de congruencia en $\mathbb{N}$. **Demostración**

Supongamos que $\sim$ es una relación de congruencia en $\mathbb{N}$ que no es la igualdad, y sea d el módulo de la congruencia $\equiv$, extensión de $\sim$ a $\mathbb{Z}$.
Dado que por definición d es el menor número natural congruente a 0 entonces por definición existe un número natural x tal que $x \sim x + d$.

Por definición w es el menor número natural que satisface que $w \sim w + d$. Para cualquier $e > w$, por ser $\sim$ una congruencia tenemos que $e - w \sim e - w$, también tenemos $w \sim w + d$ y utilizando la propiedad aditiva tenemos que $e = w + (e - w) \sim w + d + (e - w) = e + d$. Si $e = w$ entonces dado que $w \sim w + d$ entonces $e \sim e + d$. Por tanto para cualquier $e \geq w$ **(1)** entonces tenemos que $e \sim e + d$. Por tanto la clase de equivalencia de e contiene $\{e, e+d, e+2d, \cdots\}$. Así, $\overline{e} \cap \{e, e+d, e+2d, \cdots\} \neq \emptyset$, por lo tanto son iguales.

Para $u < w$, mostremos que la clase de equivalencia de u es un conjunto unitario. Supongamos que $\overline{u}$ (la clase de equivalencia de u), $\overline{u} = \{u, v, \cdots\}$ y que v es el menor miembro de $\overline{u}$ pero que excede a $w - 1$. Entonces $v > w - 1$, por lo que $v \geq w$, por **(1)** tenemos que $v \sim v + d$ y dado que $u \sim v$ y por la propiedad aditiva tenemos que $u + d \sim v + d$. Entonces $u + d \sim v + d$ y $v + d \sim v$ y $v \sim u$ entonces por

transitividad tenemos que $u + d \sim u$, es decir, $u \sim u + d$ contradiciendo la definición de w.

Así, las clases unitarias son $\{1\}, \{2\}, \cdots, \{w-1\}$, y las clases restantes son como fue dicho.

Recíprocamente, veamos que cualquier partición de $\mathbb{N}$ da una relación de congruencia en $\mathbb{N}$. Supongamos que $\mathbb{N} = \bigcup_{x \in \mathbb{N}} C_x$ y $C_x \bigcap C_y \neq \emptyset \Rightarrow C_x = C_y$.

Definamos una relación $\sim$, $a \sim b$ si y sólo si a y b pertenecen a un mismo subconjunto C_δ.

(i) $\sim$ es reflexiva. En efecto, dado que a y a pertenecen a un mismo subconjunto C_δ, $a \sim a$.

(ii) $\sim$ es simétrica. En efecto, dado que si a y b pertenecen a un mismo subconjunto C_δ (es decir, $a \sim b$) entonces b y a pertenecen a un mismo subconjunto C_δ(es decir, $b \sim a$).

(iii) $\sim$ es transitiva. En efecto, si $a \sim b$ y $b \sim c$ $\Rightarrow$ a y b pertenecen a un mismo subconjunto C_{δ_1} y b y c pertenecen a un mismo subconjunto C_{δ_2}.
Entonces $C_{\delta_1} \bigcap C_{\delta_2} \neq \emptyset$ entonces $C_{\delta_1} = C_{\delta_2}$.
Entonces a y c pertenecen a un mismo subconjunto, es decir, $a \sim c$.

Por tanto $\sim$ es una relación de equivalencia.
Ahora, veamos que $a \in C_\delta \Rightarrow \bar{a} = C_\delta$. En efecto, dado que $\bar{a} = \{x \mid x \text{ y } a \text{ están en } C_\delta\} \subset C_\delta$.
Sea $y \in C_\delta$, es decir $a \sim y$ que es lo mismo que $y \in \bar{a}$, entonces $C_\delta \subset \bar{a}$. Por tanto, $\bar{a} = C_\delta$.

Veamos que $\sim$ es una congruencia en $\mathbb{N}$.

Observación. $(p \Leftrightarrow r \wedge q \Leftrightarrow s) \leftrightarrow p \wedge q \Leftrightarrow r \wedge s$.

Veamos que $a \sim b \wedge c \sim d \Rightarrow a + c \sim b + d$, pero $a \sim b \Leftrightarrow a \in \bar{b} \wedge c \sim d \Leftrightarrow c \in \bar{d}$.

Por la **Observación** esto es equivalente a decir: $a \sim b \wedge c \sim d \Leftrightarrow a \in \bar{b} \wedge c \in \bar{d}$.
Pero $a + c \sim b + d \Leftrightarrow a + c \in \overline{b+d}$. Entonces lo que tenemos que probar es lo siguiente: $a \in \bar{b} \wedge c \in \bar{d} \Rightarrow a + c \in \overline{b+d}$.

Definamos $\overline{b+d} = \bar{b} + \bar{d}$ y $\bar{b} + \bar{d} = \{x + y \mid x \in \bar{b},\ y \in \bar{d}\}$.
Entonces si $a \in \bar{b} \wedge c \in \bar{d} \Rightarrow a + c \in \bar{b} + \bar{d} = \overline{b+d}$. Entonces $\sim$ es una relación de congruencia en $\mathbb{N}$ ■.

Observación.
Tomamos el símbolo ∞ para exceder todos los números naturales.

Notas.

(a) Las congruencias en $\mathbb{N}$ que son obtenidas por restricción de una congruencia en $\mathbb{Z}$ son las de tipo $(1, d)$.
En efecto, dado que $\mathbb{N} = \{1, 2, \cdots\}$. Como $d \equiv 0 \Rightarrow d + 1 \equiv 1 \Rightarrow d + 1 \approx 1$, 1 es el menor número natural que satisface $d + 1 \approx 1$.

(b) Es conveniente dar a la igualdad el tipo $(\infty, 0)$. En efecto, $a + 0 = a$
$\forall a \in \mathbb{N}$.

(c) El cono de cualquier anillo R tiene tipo $(1, 1)$ ver el ejemplo del anillo sin **NBI**.

Observación.
Note que los anillos con **NBI** son precisamente los de tipo $(\infty, 0)$. En efecto, Si R tiene **NBI** entonces la relación $\sim_R$ es simplemente la igualdad $(=)$ y dado que la igualdad tiene tipo $(\infty, 0)$. Entonces R tiene tipo $(\infty, 0)$.

Sea $f: R \longrightarrow S$ un homomorfismo de anillos. Si $a \sim_R b$ entonces $a \sim_S b$. **Demostración**

Si $a \sim_R b$ entonces por definición existe una matriz invertible P de tamaño $a \times b$ sobre R entonces por proposición tenemos que $f(P)$ es una matriz invertible de tamaño $a \times b$ sobre S, es decir $a \sim_S b$. ■

Si $a \sim_R b \Rightarrow a \sim_S b$, entonces decimos que $\sim_R$ es *más fina* que $\sim_S$.

Sea $\sim_R$ *más fina* que $\sim_S$. Para $z \in [x]_S$ entonces $[z]_R \subseteq [x]_S$. **Demostración**

Sea $y \in [z]_R$ entonces $y \sim_R z$, entonces $y \sim_S z$ pués $\sim_R$ es *más fina* que $\sim_S$, pero $z \sim_S x$ entonces $y \sim_S x$, es decir $y \in [x]_S$. Por tanto $[z]_R \subseteq [x]_S$. ■

(w,d) y (u,c) son los respectivos tipos de R y S, además si $\sim_R$ es *más fina* que $\sim_S$, entonces $u \leq w$ y c divide a d $(c \mid d)$. **Demostración**

Veamos que $u \leq w$. Razonando por el absurdo, supongamos que $u > w$ entonces $u - 1 > w - 1$ entonces $\{u-1\} \neq \{k\}, k = 1, 2, \cdots, w-1$.
Entonces por el **Teorema 3.1**, $\{u-1\}$ es una $\sim_R$-clase de equivalencia infinita **(absurdo)**. Entonces $u \leq w$.
Veamos que c divide a d. Dado que $u \leq w$, entonces existe $k \in \mathbb{N}$ tal que $u + k = w$. Así, $[u+k]_S = [w]_S$, como $\sim_R$ es *más fina* que $\sim_S$ entonces $[w]_R \subseteq [w]_S$ y en consecuencia $[w]_R \subseteq [u+k]_S$, así $\{w, w+d, w+2d, \cdots\} \subseteq \{u+k, u+k+c, \cdots\} = \{w, w+c, w+2c, \cdots\}$. Entonces ó $w + d = w + c$ ó existe $r \in \mathbb{N}$ tal que $w + d = w + rc$.

En el primer caso, $d = c$ y c es divisor de d. En el segundo caso, $w + d = w + rc$ y por lo tanto $d = rc$ para algún r; así c es divisor de d.

Sean R y S anillos y supongamos que (w,d), (w',d') son los respectivos tipos de R y S. Si $R \approx S \Rightarrow w = w'$ y $d = d'$. **Demostración**

Dado que $R \approx S$ entonces existe $\psi : R \to S$ tal que ψ es un homomorfismo de anillos y ψ^{-1} es un homomorfismo de anillos. Por proposición tenemos que $\sim_R$ es más fina que $\sim_S$ pues $\psi : R \to S$ es un homomorfismo de anillos y también tenemos que $\sim_S$ es más fina que $\sim_R$ pues $\psi^{-1} : S \to R$ es un homomorfismo de anillos. Dado que (w,d), (w',d') son los respectivos tipos de R y S y $\sim_R$ es más fina que $\sim_S$ entonces por la proposición anterior tenemos que $w' \leq w$ y $d' \mid d$. Análogamente, dado que (w,d), (w',d') son los respectivos tipos de R y S y $\sim_S$ es más fina que $\sim_R$ entonces por la proposición anterior tenemos que $w \leq w'$ y $d \mid d'$. Entonces $w = w'$ y $d = d'$. ■

(w,d) y (u,c) son los respectivos tipos de las congruencias $\sim$ y $\approx$ en $\mathbb{N}$, y si $u \leq w$ y c divide a d, entonces $\sim$ es *más fina* que $\approx$. **Demostración**

Dado que $u \leq w$ y c divide a d, entonces $w = u + k$ para algún $k \in \mathbb{N}$ y $d = rc$ para algún $r \in \mathbb{N}$. Las clases de equivalencia de $\sim$ son:
$\overline{1}_\sim = \{1\}, \cdots, \overline{w-1}_\sim = \{w-1\}$ y $\overline{e}_\sim$, donde $e = w, w+1, \cdots, w+d-1$
Las clases de equivalencia de $\approx$ son:
$\overline{1}_\approx = \{1\}, \cdots, \overline{u-1}_\approx = \{u-1\}$ y $\overline{t}_\approx$, donde $t = u, u+1, \cdots, u+c-1$.
Pero $w = u + k$ y $d = rc$, por tanto las clases de equivalencia de $\sim$ son:
$\overline{1}_\sim = \{1\}, \cdots, \overline{u+k-1}_\sim = \{u+k-1\}$ y $\overline{e}_\sim$, donde $e = u+k, u+k+1, \cdots, u+k+rc-1$.
Las clases de equivalencia de $\approx$ son:
$\overline{1}_\approx = \{1\}, \cdots, \overline{u-1}_\approx = \{u-1\}$ y $\overline{t}_\approx$, donde $t = u, u+1, \cdots, u+c-1$.

Vemos que $\overline{1}_\sim = \overline{1}_\approx, \cdots, \overline{u-1}_\sim = \overline{u-1}_\approx$.
$\{u\} = \overline{u}_\sim \subseteq \overline{u}_\approx$, también $\{u+k-1\} = \overline{u+k-1}_\sim \subseteq \overline{u+k-1}_\approx = \{u+k-1, u+k-1+c, \cdots\}$.
Veamos que las clases infinitas también satisfacen que $\overline{e}_\sim \subseteq \overline{e}_\sim$.
En efecto, $\overline{e}_\sim = \{e\} \cup \{e+\delta rc \mid \delta \in \mathbb{N}\}$ y $\overline{e}_\approx = \{e\} \cup \{e+nc \mid n \in \mathbb{N}\}$.
Sea $y \in \overline{e}_\sim$, entonces $y = e+\delta rc$, para algún $\delta \in \mathbb{N}$. Entonces $y = e + \overbrace{(\delta r)}^{n} c$, es decir, $y \in \overline{e}_\approx$.
Dado que toda clase de equivalencia de $\sim$ está contenida en al menos una clase de equivalencia de $\approx$ se tiene que, $\sim$ es *más fina* que $\approx$. En efecto, si $x \sim y$ entonces $x \in \overline{y}_\sim \subseteq \overline{y}_\approx$ entonces $x \approx y$. ■

Supongamos que hay un homomorfismo de anillos de R a S, $f: R \longrightarrow S$. Supongamos que S tiene **NBI**, entonces R tiene **NBI**. **Demostración**
Supóngase que (w,d) es el tipo de R, como S es de tipo $(\infty,0)$ y como hay un homomorfismo de anillos esto implica que $\sim_R$ es *más fina* que $\sim_S$ entonces por proposición, tenemos que $\infty \leq w$ y 0 es divisor de d entonces $w = \infty$ y $d = 0$, es decir, el tipo de R es $(\infty,0)$ entonces R tiene **NBI**. ■

Observación.
No hay razón para que exista un homomorfismo de un anillo R a un anillo S cuando $\sim_R$ es *más fina* que $\sim_S$. Por ejemplo, no existe homomorfismo entre los campos finitos $\mathbb{F}_p$ y $\mathbb{F}_q$, $p \neq q$.
$f: \mathbb{F}_p \longrightarrow \mathbb{F}_q$, f es un homomorfismo, $f(\overline{0}) = \overline{0}$ y $f(\overline{1}) = \overline{1}$.
Supongamos que $p < q$, la clase $\overline{q-p}$ pertenece a $\mathbb{F}_q$ pués $0 < q-p < q$.
$f(\overline{p}) = f(\overline{0}) = \overline{0}$.

$$
\begin{aligned}
f(\overline{p}) &= f(\overline{1} + \overbrace{\cdots}^{p-veces} + \overline{1}) \\
&= f(\overline{1}) + \overbrace{\cdots}^{p-veces} + f(\overline{1}),\ f\ es\ un\ homomorfismo \\
&= pf(\overline{1}) \\
&= p\overline{1} \\
&= \overline{p}
\end{aligned}
$$

Entonces $\overline{p} = \overline{0}$ en $\mathbb{F}_q$ (**absurdo**), por tanto no existe un homomorfismo de $\mathbb{F}_p$ a $\mathbb{F}_q$. Dado que $\mathbb{F}_p$ y $\mathbb{F}_q$ son campos entonces tienen **NBI** y por tanto tienen tipo $(\infty,0)$. Supóngase que $(\infty,0)$ son los respectivos tipos de las congruencias $\sim$ y $\approx$ en $\mathbb{N}$ y por lo que vimos anteriormente $\sim$ es *más fina* que $\approx$. ■

Ejemplo
Supongamos que $D = R_1 \times R_2$, el producto directo de anillos, y R_1 y R_2 tienen tipo (w_1,d_1) y (w_2,d_2) respectivamente. Entonces D tiene tipo $(min(w_1,w_2), mcm(d_1,d_2))$, donde *mcm* significa mínimo común múltiplo.

Demostración

Sean $\sim$ una relación de congruencia en $\mathbb{N}$ y $\equiv$ una congruencia en $\mathbb{Z}$ por la extensión de $\sim$ a $\mathbb{Z}$. En D definimos $(x,y) \sim (u,v) \Leftrightarrow x \sim u \wedge y \sim v$ y $(z_1,z_2) \equiv (z_1',z_2') \Leftrightarrow z_1 \equiv z_1' \wedge z_2 \equiv z_2'$, esto es una congruencia en $\mathbb{N}$. Dado que existen $x \in \mathbb{N}$ y $y \in \mathbb{N}$ tales que $d_1 + x \sim x$ y $d_2 + y \sim y$. Entonces $d_1 + (d_1 + x) \sim d_1 + x \wedge d_1 + x \sim x \Rightarrow 2d_1 + x \sim x$, análogamente $2d_2 + y \sim y$, por inducción se prueba que $\forall k \in \mathbb{N}$, $kd_1 + x \sim x \wedge kd_2 + y \sim y$. Si $d \in \mathbb{N}$ y cumple $d + x \sim x \wedge d + y \sim y$ y d es el mínimo que satisface las dos condiciones anteriores, entonces $d = k_1d_1$ y $d = k_2d_2$, para algunos $k_1, k_2 \in \mathbb{N}$, es decir d es múltiplo común de d_1 y d_2; luego $d = mcm(d_1,d_2)$. Ahora como w_1 es el mínimo que satisface $w_1 + d_1 \sim w_1$ y w_2 es el mínimo que satisface $w_2 + d_2 \sim w_2$. Buscamos el mínimo w tal que $w + d \sim w$, sabiendo que $w_1 + d_1 \sim w_1$ y $w_2 + d_2 \sim w_2$, entonces $w_1 + d \sim w_1$ y $w_2 + d \sim w_2$.

Si $w = w_1 \Rightarrow w_1 + d \sim w_1 \Rightarrow w + d \sim w$.

Si $w = w_2 \Rightarrow w_2 + d \sim w_2 \Rightarrow w + d \sim w$.

En consecuencia, si tomamos $w = min(w_1, w_2)$, se satisface $w + d \sim w$.

5. Conclusiones

- Existen matrices rectangulares invertibles en el sentido definido anteriormente.
- A diferencia de espacios vectoriales de dimensión finita, en donde cualesquier par de bases en un mismo espacio vectorial, tienen el mismo número de elementos(Dimensión del espacio vectorial), en R-módulos puede suceder que existan bases para el mismo R-módulo con distinto número de elementos, a menos que tenga la condición de **NBI**.

Referencias

[1] A. J. Berrick and M. E. Keating, *Rectangular Invertible Matrices*.

[2] M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, Mass. 1969.

[3] G. M. Bergman, Coproducts and some universal ring constructions, *Trans. Amer. Math. Soc.* **200** (1977), 33-88.

[4] P. M. Cohn, Some remarks on the invariant basis property, *Topology* **5** (1966), 215-228.

[5] P. M. Cohn, *Algebra II*, Wiley & Sons, Chichester, 1977.

[6] P. M. Cohn, *Universal Algebra*, Reidel, Dordrecht, 1981.

[7] P. M. Cohn, *Algebra I*, Wiley & Sons, Chichester, 1982.

[8] K. Goodearl, P. Menal, and J. Moncasi, Free and residually artinian regular rings, J. Algebra **156** (1993), 407-432.

[9] J. M. Howie, *An Introduction to Semigroup Theory*, London Math. Soc. Monograph 7, Academic Press, London, 1976.

[10] W. van der Kallen, Injective stability for K_2, *Lecture Notes in Math.* **551**, Springer, Berlin, 1976, pp.77-154.

[11] W. G. Leavitt, Modules without invariant basis number, *Proc. Amer. Math. Soc.* **8** (1957), 322-328.

[12] W. G. Leavitt, The module type of a ring, *Trans. Amer. Math. Soc.* **103** (1962), 113-130.

[13] W. G. Leavitt, The module type of a homomorphic image, *Duke Math. J.* **32** (1965), 305-311.

[14] L. N. Vaserstein , Stable ranks of rings and dimensionality of topological spaces, *Funct. Anal. And Appl.* **5** (1971), 102-110.

[15] Lous H. Rowen, Ring Theory, Volume I, **1.3** p. 61.

Para citar este artículo: German Gómez et al . 2014, "Matrices Rectangulares Invertibles". Disponible en Revistas y Publicaciones de la Universidad del Atlántico en http://investigaciones.uniatlantico.edu.co/revistas/index.php/MATUA.