El Lema de Zorn y algunas aplicaciones

Carina Boyallian - Gabriela Ovando

Biografía

Max August Zorn nació el 6 de junio de 1906 en Krefeld, Alemania, hijo de Theodor Maximilian Wilhem y Anna Katherina (Nissen) Zorn.

Fue educado en Hamburgo, donde obtuvo el título de bachiller en 1923. En 1930 se doctoró en la Universidad de Hamburgo, consiguió un cargo en la Universidad de Halle (1930-1931) y luego se desempeñó en la Universidad de Hamburgo hasta 1933. En 1934, como consecuencia de su negativa de adhesión al régimen nazi, dejó Alemania con su esposa Alice y su hijo de 3 años, emigrando a los E.E.U.U.. Así, mientras trabajaba en la Universidad de Yale con una beca Sterling, produjo el conocido Lema de Zorn, fundamental en el desarrollo de la matemática. Desde 1936 hasta 1946 fue profesor en la Universidad de los Ángeles. Entre 1946 y 1971 fue profesor en la Universidad de Indiana. En este período obtuvo el título de profesor emérito en dicha Universidad.

Fue miembro de la American Mathematical Society, Mathematical Association of America , Association for Symbolic Logic, Sigma Epsilon y Sigma Xi.

Max Zorn murió el martes 9 de marzo de 1993 por una complicación cardíaca. Nunca se recuperó completamente después de ser atropellado por un automóvil el 26 de noviembre del año anterior, cuando salía de la Universidad de Indiana con rumbo a su casa.

Lema de Zorn.

Sea C un conjunto. Una relación binaria $\preceq$ en C se dice *orden* si se satisfacen:

$$\left.\begin{array}{ll} 1) & a \preceq a \\ 2) & a \preceq b,\ b \preceq c \Longrightarrow a \preceq c \\ 3) & a \preceq b \ \ y \ \ b \preceq a \Longrightarrow a = b \end{array}\right\} \textit{Axiomas de orden}$$

Si se satisface 1), 2) y 3), entonces se trata de una relación reflexiva, transitiva y antisimétrica.

Luego $(C, \preceq)$ se dice que es un conjunto *parcialmente ordenado.*

Si $x, y \in C$ y $x \preceq y$ se dice que x *precede a* y.

Si dados $x, y \in C$ se cumple que $x \preceq y$ ó $y \preceq x$ entonces x e y se dicen *comparables.*

$(C, \preceq)$ se dice que es un conjunto *totalmente ordenado* si todos sus elementos son comparables.

Ejemplos

i) De conjuntos parcialmente ordenados:

Sea

$$U = \{\ 1, 2, 3, 4\ \}$$

y sea $\mathbf{B}$ la famila de subconjuntos de U, i.e.:

$$\begin{aligned} \mathbf{B} = \ & \{\varnothing, U, \\ & \{1\}, \{2\}, \{3\}, \{4\}, \\ & \{1,2\}, \{1,3\}, \{1,4\}, \{2,4\}, \{3,4\}, \{2,3\} \\ & \{1,2,3\}, \{1,3,4\}, \{2,3,4\}, \{1,4,2\}\} \end{aligned}$$

Démosle a $\mathbf{B}$ el orden de la inclusión, o sea si $A \in \mathbf{B}$ y $B \in \mathbf{B}$ entonces $A \preceq B$ si $A \subseteq B$, i.e. tenemos $(\mathbf{B}, \subseteq)$. Se puede verificar fácilmente que esta relación satisface los axiomas de orden. Luego diremos $\{1\} \preceq \{1,2\}$, ó $\{2,3\} \preceq \{2,3,4\}$ pues $\{1\} \subseteq \{1,2\}$ ó $\{2,3\} \subseteq \{2,3,4\}$.

Pero notemos que no todos sus elementos son comparables, por ejemplo $\{1\}$ con $\{2\}$ ó $\{2.3\}$ con $\{3.4\}$. Por lo tanto $(\mathbf{B}, \subseteq)$ es un conjunto *parcialmente ordenado.*

ii) De conjuntos totalmente ordenados:

I) $(\mathbf{N}, \leq)$, donde $\leq$ es el orden usual de los números naturales.

II) $(\mathbf{R}, \leq)$, donde $\leq$ es el orden usual de los números reales.

III) Sea A el conjunto de los pares ordenados de números naturales (m, n).

Definamos en A el siguiente orden:

Diremos que $(m, n) \preceq (r, s)$ si $m < r$, y si $m = r$ entonces $n \leq s$

Observemos que dos pares ordenados son iguales con este orden si y sólo si sus coordenadas son iguales. Además notemos que dados dos pares ordenados cualesquiera son comparables, por ejemplo :

$$(13, 124) \preceq (13, 786) \quad y \quad (1243, 456) \preceq (3435, 1)$$

Este es un *orden total*, llamado el orden *lexicográfico.* Se puede extender a n-uplas de números reales. Observemos que el orden lexicográfico es similar al orden alfabético, digamos que una palabra es menor que otra si aparece antes en el diccionario.

Diremos que $M \in (C, \preceq)$ es *máximo elemento* si M sigue a todo elemento de C, i.e., $M \succeq c. \forall \ c \in C$.

Análogamente, definimos como *mínimo elemento* de C, un $m \in C$ tal que $m \preceq c, \quad \forall\ c \in C$.

Notemos que si tales elementos existen son únicos. Pero no siempre existen elementos máximos o mínimos, por ejemplo, en $(\mathbf{N}, \leq)$, no existe máximo elemento.

Volvamos por un instante al ejemplo *i)*. Notemos que U es un elemento máximo. Pero hay en $\mathbf{B} \sim \{U\}$ (ordenado con la inclusón) elementos tales que ningun otro elemento de $\mathbf{B} \sim \{U\}$ lo contiene estrictamente, por ejemplo

$$\{1,2,3\},\ \{1,3,4\},\ \{2,3,4\},\ \{1,4,2\}$$

Estos elementos son llamados elementos maximales de $\mathbf{B}$. Generalicemos esta idea.

Definición: Sea $(C, \preceq)$ un conjunto parcialmente ordenado. Diremos que $M \in (C, \preceq)$ es un *elemento maximal* si para todo c comparable con M , $c \preceq M$.

Análogamente, se define *elemento minimal* como un elemento de C tal precede a todo elemento comparable con él.

Notemos que si consideramos $C = \{\{1\},\{2\},\{3\},\{4\}\}$ y lo ordenamos con la inclusión todos sus elementos son maximales, y si tomamos C como los reales con el orden usual no existen elementos maximales.

Luego cabe preguntarse, cuándo $(C, \preceq)$ tiene elementos maximales. La respuesta a esta pregunta está dada por el lema de Zorn.

Definición: Sea $(C, \preceq)$ un conjunto parcialmente ordenado. Diremos que un subconjunto η de C es una *cadena* si todos los elementos de η son comparables, i.e. si $a \in \eta$ y $b \in \eta$ entonces $a \preceq b$ o bien $b \preceq a$.

Observación: Los elementos de la cadena pueden ser familias de conjuntos. Aclaremos esto con el siguiente

Ejemplo:

Volvamos al ejemplo *ii.*

$$\begin{aligned}\mathbf{B} = \quad & \{\varnothing, \quad U, \\ & \{1\}, \{2\}, \{3\}, \{4\}, \\ & \{1,2\}, \{1,3\}, \{1,4\}, \{2,4\}, \{3,4\}, \{2,3\} \\ & \{1,2,3\}, \{1,3,4\}, \{2,3.4\}. \{1,4,2\}\}\end{aligned}$$

Recordemos que habíamos considerado B ordenado con la inclusión.

Cadenas de este conjunto serían, por ejemplo:

$$\begin{aligned}\eta = \quad & \{\{1\}, \{1,2\}, \{1,2,3\}, \{1,2,3,4\}\} \\ \eta' = \quad & \{\varnothing \quad \{2,3\}, \{2,3,4\}\} \\ \eta'' = \quad & \{\{4\}\}\end{aligned}$$

Consideramos, ahora, la colección de todas las cadenas de una familia parcialmente ordenada F. Dadas η y μ dos cadenas de F diremos que $\eta \preceq \mu$ si todo elemento de η está en μ.

Luego nos podríamos preguntar si existe una cadena maximal.

Tomemos el siguiente axioma, que contesta esta pregunta.

PRINCIPIO DE MAXIMALIDAD DE HAUSSDORFF

Sea F un conjunto parcialmente ordenado. Entonces dada una cadena η de F existe μ, cadena maximal tal que $\eta \preceq \mu$.

Deduzcamos ahora el lema de Zorn.

LEMA DE ZORN. Sea F un conjunto parcialmente ordenado tal que toda cadena de F tiene cota superior, i.e. para cada μ cadena en F $\exists a \in F$ tal que $m \preceq a \ \forall \ m \in \mu$. Entonces existe un elemento maximal en F.

Demostración: El principio de maximalidad de Hausdorff, garantiza la existencia de una cadena maximal μ. Por hipótesis existe una cota superior $a \in F$ de la cadena maximal μ, i.e. $m \preceq a \ \forall m \in \mu$. Luego a es un elemento maximal de F.

Supongamos que no lo fuera, por lo tanto $\exists \ b \in F$ tal que $a \preceq b$. Consideremos ahora la cadena

$$\mu' = \mu \ \cup \ \{b\}$$

Pero $\mu \ \preceq \ \mu'$, lo cual es un absurdo, pues μ era una cadena maximal.□

Veamos ahora ejemplos de aplicaciones del Lema de Zorn.

Ejemplo I:

Consideremos el conjunto de los números naturales $\mathbf{N}$ y consideremos la siguiente familia de subconjuntos de $\mathbf{N}$

$$F = \{A \subseteq \mathbf{N} : \ si \ x \in A, \ y \in A \ entonces \ xy \ es \ par \ \}.$$

Ordenemos esta familia con la inclusión.

Notemos que $F \neq \emptyset$ pues el conjunto de los números pares pertenece a F.

Sea $\eta = \{C_i : i \in I\}$ una cadena de η, donde I es una familia de subíndices. Para aplicar el Lema de Zorn, deberíamos verificar que esta cadena tiene una cota superior. Sea

$$M = \bigcup_{i \in I} C_i$$

Claramente $M \succeq C_i \ \forall \ i \in I$. Faltaría verificar que $M \in F$.

Tomemos x e y en M , luego por la definición de M , $x \in C_i$ para algún $i \in I$ y $y \in C_j$ para algún $j \in I$. Como C es una cadena, $C_i \subseteq C_j$ ó bien $C_j \subseteq C_i$. Supongamos que $C_i \subseteq C_j$. Luego $x \in C_j$, por lo tanto xy es par pues $C_j \subset F$.

Así, tenemos que toda cadena de F tiene cota superior. Por el Lema de Zorn tenemos que existe un elemento maximal en F.

Veamos cómo son esos elementos maximales. Observemos que el conjunto de todos los números pares, que denotaremos por P, debe estar contenido en el elemento maximal, pues de lo contrario no sería maximal.

Además, un elemento maximal puede contener sólo un número impar pues si hubiera más de uno el producto entre ellos daría un número impar.

Luego los elementos maximales de F serán

$$M_k = P \cup \{2k+1\} \qquad k \in \mathbf{Z}$$

Observemos que no hay un único elemento maximal.

Ejemplo II:

Consideremos ahora, **E** un espacio vectorial sobre un cuerpo K.

Recordemos que un subconjunto A de **E** se dice *linealmente independiente* (l.i) si y solo si cualquier combinación lineal finita de elementos de A, i.e.

$$\sum_{i=1}^{N} a_i x_i \quad con\ x_i \in A \quad \forall\ i = 1.....N, \quad y\ con \quad x_i \neq x_k\ si\ i \neq k$$

es igual a 0 solo si cada a_i es igual a 0.

Esto, es equivalente a decir que si un elemento de **E** puede ser escrito como una combinación lineal de distintos elementos de A con coeficientes no nulos, esta representación es única, pues de lo contrario A no sería linealmente independiente.

Un subconjunto B de **E** es una *Base de Hamel* si y solo si cada elemento no nulo de **E** puede ser representado de manera única como una combinación lineal finita de elementos de B con coeficientes no nulos.

Una base de Hamel es necesariamente linealmente independiente. Nos preguntamos si **R** como **Q**-espacio vectorial tiene una base de Hamel. La respuesta es sí y la da el Lema de Zorn.

Sea

$$L = \{A \subseteq \mathbf{R} \ :\ A\ es\ un\ subconjunto\ l.i.\ de\ \mathbf{R} \quad \}$$

Observemos que L es no vacío, pues si $a \in \mathbf{R}$, entonces $\{a\}$ es l.i. . Diremos que $A_1 \preceq A_2$, si A_1 está contenida en A_2.

Queremos ver que un elemento maximal de L es una base de Hamel.

Sea $C = \{C_i : i \in I\}$ una cadena en L. Deberíamos ver que C tiene una cota superior. Sea $S = \cup C_i$. Claramente $C_i \subseteq S \quad \forall i \in I$. Luego, solo nos faltaría ver que $S \in L$. Sean $x_1, x_2, ..., x_n$ elementos de S tales que $x_i \neq xj$ si $i \neq j$, pero para algún $i_0 \in I$, x_i está en $C_{i_0} \quad \forall\, i = 1.....n$, pues C es una cadena, por lo tanto son l.i., y así S es cota superior de C. El Lema de Zorn nos dice que existe un elemento maximal H. Veamos que H es una base de Hamel.

Supongamos que no lo sea, por lo tanto existe $y \in \mathbf{R}, \quad y \neq 0$ tal que no tiene la representación como combinación lineal finita de elementos de H. Consideremos ahora el conjunto $H \cup \{y\}$. Este conjunto está en L y contiene a H, pero esto es un absurdo ya que H es maximal.

Desde hace tiempo, los hombres se han preocupado por medir ciertas cosas que lo rodean. Esto significa, elegir bajo algún criterio, cierto patrón para caracterizar una propiedad determinada del objeto a medir. Por ejemplo se puede medir la longitud de una varilla, o su peso. Los objetos a medir pueden ser concretos o abstractos, y pertenecer a áreas muy diversas. La matemática no ha quedado ausente en las necesidades humanas y ha elaborado la llamada teoría de la medida, sobre objetos matemáticos. Por ejemplo a los siguientes conjuntos:

$$\begin{aligned} I &= \{x \in \mathbf{R} : a < x < b\} = (a,b) && \text{intervalo abierto} \\ I' &= \{x \in \mathbf{R} : a \leq x < b\} = [a,b) && \text{intervalo semi-abierto} \\ I'' &= \{x \in \mathbf{R} : a \leq x \leq b\} = [a,b] && \text{intervalo cerrado} \end{aligned}$$

la medida que se les asigna es su longitud, i.e. $l(I) = b - a$.

La longitud es un ejemplo de una función conjunto, esto es una función que asocia un número real extendido(i.e. un número de $\mathbf{R} \cup \{\infty\}$) a cada conjunto de una colección de conjuntos. En nuestro caso el dominio de la

función longitud es el conjunto de todos los intervalos. Se quiere extender esta noción de longitud a otros conjuntos más complicados de $\mathbf{R}$, o sea definir una función de conjunto m, que asigne a cada conjunto E de una colección M de conjuntos de números reales un número real extendido. Idealmente quisieramos que m satisfaga la siguientes propiedades:

i) mE esté definida para cualquier subconjunto de números reales, i.e. que $M = P(\mathbf{R})$.

ii) Para un intervalo I, $mI = l(I)$.

iii) $m(E) = m(E + a) \quad \forall\, a \in \mathbf{R}$, es decir que sea invariante por traslaciones.

iv) Si $\{E_n\}_{n=1}^{\infty}$ es una sucesión en M de conjuntos disjuntos , entonces $m(\cup\, E_n) = \sum E_n$.

Pero no es posible que una función medida satisfaga las cuatro propiedades simultaneamente. Veremos, por ejemplo, el caso de la llamada medida de Lebesgue que satisface las tres últimas propiedades pero no la primera, usando para ello las bases de Hamel.

Sea A un subconjunto arbitrario de $\mathbf{R}$. Un cubrimiento numerable de A por intervalos abiertos es una familia $\{I_n\}_{n=1}^{\infty}$ de intervalos abiertos tales que

$$A \subseteq \bigcup_{i=1}^{\infty} I_n.$$

Definición: Sea A un subconjunto de números reales. Definimos como la *medida exterior de* A a:

$$m^*(A) = inf\{\sum_{i=1}^{\infty} l(I_n) \ : \{I_n\}_{i=1}^{\infty} \textit{ es un cubrimiento por abiertos de } A\}.$$

La $m^* : P(\mathbf{R}) \longrightarrow \mathbf{R}_{\geq 0}$ es una aplicación que satisface las siguientes propiedades:

i) Si $A \subseteq B$, entonces $m^*(A) \leq m^*(B)$.

ii) Si I es un intervalo, entonces $m^*(I) = l(I)$.

iii) m^* es invariante por traslaciones, i.e. $m^*(A) = m^*(A+c)$ *con* $c \in \mathbf{R}$.

Probemos la siguiente proposición:

Proposición: Sea $\{A_n\}_{n=1}^{\infty}$ una familia numerable de subconjuntos de $\mathbf{R}$. Entonces

$$m^*(\bigcup_{i=1}^{\infty} A_n) \leq \sum_{i=1}^{\infty} m^*(A_n).$$

Demostración: Para cada n, dado $\frac{\epsilon}{2^n}$, existe por definición de medida exterior un cubrimiento $\{I_i^n\}_{i=1}^{\infty}$ de cada A_n que satisface la siguiente desigualdad:

$$m^*(A_n) + \frac{\epsilon}{2^n} \geq \sum_{i=1}^{\infty} l(I_i^n) \quad (*)$$

Observemos que como cada $\{I_i^n\}_{i=1}^{\infty}$, es un cubrimiento de cada A_n, entonces la $\cup_n \cup_i I_i^n \subseteq \cup_n A_n$, y por lo tanto $\{I_i^n\}_{i,n=1}^{\infty}$ es un cubrimiento de $\cup_n A_n$.

Luego, por $(*)$

$$m^*(\bigcup_{n=1}^{\infty} A_n) \leq \sum_{n,i=1}^{\infty} l(I_i^n) \leq \sum_{n=1}^{\infty} m^*(A_n) + \epsilon.$$

Como ϵ era arbitrario,tenemos probada la proposición. □

Definición: Diremos que un conjunto E es *medible* si $\forall\, A \subseteq \mathbf{R}$

$$m^*(A) = m^*(A \cap E) + m^*(A \cap E^c)$$

donde E^c denota E complemento.

Veremos que existen conjuntos no medibles, usando que $\mathbf{R}$ como $\mathbf{Q}$-espacio vectorial tiene una base de Hamel.

Como consecuencia de la definición de conjunto medible tenemos los siguientes resultados:

i) Si E_1 y E_2 son medibles, entonces $E_1 \cup E_2$ es medible.

ii) Si $E_1, E_2, ..., E_n$ son conjuntos disjuntos medibles y A es un conjunto arbitrario, entonces

$$m^*(A \cap [\cup_{i=1}^n E_i]) = \sum_{i=1}^n m^*(A \cap E_i).$$

Usando i) y ii) se demuestra que si $\{E_n\}_{n=1}^{\infty}$ es una familia numerable de conjuntos medibles entonces la $\cup_{n=1}^{\infty} E_n$ es medible, y además, si esta familia los E_i son disjuntos dos a dos entonces

$$m^*(\bigcup_{n=1}^{\infty} E_n) = \sum_{i=1}^{\infty} m^*(E_n)$$

Probemos esta última afirmación. La proposición anterior nos da una desigualdad. Tratemos de obtener la otra. Si en la propiedad ii) consideramos ese conjunto A como $\mathbf{R}$, tenemos que para cada n fijo

$$m^*(\bigcup_{n=1}^{n} E_n) = \sum_{i=1}^{n} m^*(E_i)$$

Luego, como $\cup_{i=1}^n E_i \subseteq \cup_{i=1}^{\infty} E_i \ \forall n$ tenemos que

$$m^*(\bigcup_{i=1}^{\infty} E_i) \geq m^*(\bigcup_{i=1}^{n} E_i) = \sum_{i=1}^{n} m^*(E_i)$$

Como el término de la izquierda no depende de n, tenemos que

$$m^*(\bigcup_{i=1}^{\infty} E_i) \geq \sum_{i=1}^{\infty} m^*(E_i)$$

Ahora con todos estos resultados estamos en condiciones de comenzar la construcción de un conjunto no medible.

Empecemos definiendo la *suma módulo uno* en el intervalo $[0,1)$.

Sean x e y en el $[0,1)$

$$x +, y = \begin{cases} x+y, & si\ x+y \leq 1 \\ x+y-1, & si\ x+y \geq 1 \end{cases}$$

Ahora, si E es un conjunto medible contenido en el [0,1), entonces se puede ver que $E + c$ es medible y que $m^*(E + c) = m^*(E)\ \forall\ c \in \mathbf{R}$

Definamos una relación de equivalencia. Diremos que $x \sim y$ si $x - y \in \mathbf{Q}$. Sean $x \sim y$. Como $\mathbf{R}$ tiene una base de Hamel H como $\mathbf{Q}$-espacio vectorial , entonces existen $x_1 \neq x_2 \neq ..... \neq x_n$ en H y $q_0, q_1, ...q_n$ en $\mathbf{Q}$ tales que $x = q_0 + q_1x_1 + ... + q_nx_n$ y también existen $y_1 \neq y_2 \neq ..... \neq y_m$ en H y $r_0, r_1, ...r_m$ en $\mathbf{Q}$ tales que $y = r_0 + r_1y_1 + ... + r_my_m$.

Ahora,

$$\begin{aligned} x - y = \ & (q_0 + q_1x_1 + ... + q_nx_n) - (r_0 + r_1y_1 + ... + r_my_m) \\ & (q_0 - r_0) + (q_1x_1 + ... + q_nx_n) - (r_1y_1 + ... + r_my_m)) \end{aligned}$$

Como $x \sim y$, entonces $x - y \in \mathbf{Q}$. Luego

$$(q_1x_1 + ... + q_nx_n) - (r_1y_1 + ... + r_my_m)) \in \mathbf{Q}$$

pues $q_0 - r_0 \in \mathbf{Q}$. Pero esto es una contradición, a menos que $m = n$ y que para cada i $x_i = y_k$ y $q_i = r_k$ para algún k

Consideremos ahora como

$$\begin{aligned} P = \ & \{x \in [0,1) : \exists\ x_1 \neq x_2 \neq ..... \neq x_n\ en\ H\ y\ q_0, q_1, ...q_n\ en\ \mathbf{Q} \\ & tales\ que\ x = q_0 + q_1x_1 + ... + q_nx_n,\ con\ q_0 = 0\} \cup \{0\} \end{aligned}$$

Sea $\{r_i\}_{i=1}^{\infty}$ una enumeración de los racionales de $[0,1)$, con $r_0 = 0$, y definamos $P_i = P + r_i$.

Así $P_0 = P$. Notemos que $\cup P_i = [0,1)$, pues sea $x \in [0,1)$ entonces x va a diferir de algún elemento de P en un racional, por lo tanto está en algún P_i

Además, $P_i \cap P_k = \varnothing$ si $i \neq k$, pues si suponemos que existe $x \in P_i \cap P_k$, entonces $x = p + r_i = m + r_k$ con $p, m \in P$. Por lo tanto, $p - m \in \mathbf{Q} \cap P$, luego $p = m$ y así $r_i = r_k$, lo que es una contradicción.

P es un conjunto no medible

Probemos esta afirmación. Supongamos que sea medible, por lo tanto, como cada $P_i = P + r_i$, también es medible, y $m^*(P_i) = m^*P)$.

Así, como $\cup P_i = [0,1)$ y $P_i \cap P_k = \varnothing$ si $i \neq k$,tenemos

$$1 = m^*[0,1) = m^*(\bigcup_{i=1}^{\infty} P_i) = \sum_{i=1}^{\infty} m^*(P_i) = \sum_{i=1}^{\infty} m^*(P)$$

Pero si $m^*(P) > 0$ esto me diriá $1 = \infty$ y si $m^*(P) = 0$ entonces 1=0. Absurdo que provino de suponer que P era medible

Ejemplo III:

Consideremos un anillo R conmutativo, y sea S un subconjunto no vacío de R que es cerrado para las operaciones del anillo R, i.e. un subanillo.

Un subanillo I de R se dice *ideal* si

$$r \in R \ \ y \ \ x \in I \quad \Longrightarrow \quad rx \in I$$

Diremos que un ideal M es *maximal* si $M \neq R$ y para todo ideal N tal que $M \subseteq N \subseteq R$, $N = R$, ó bien $N = M$. Observemos que

M maximal implica que $1_R \notin R$, pues si $r \in R$ y $1_R \in M$, entonces $M = R$.

Supongamos ahora que $R \neq \{0\}$, donde $\{0\}$ es el ideal cuyo único elemento es el 0, y tiene identidad, i.e. $\exists\, 1_R \in R$, tal que $r1_R = r \ \forall\, r \in R$. Entonces en R siempre existe un ideal maximal, de hecho, *todo ideal I en R está contenido en un ideal maximal.*

Pues:

Como $\{0\}$ es un ideal de R, y $R \neq \{0\}$, basta con probar la segunda afirmación.

Sea $A \neq R$ un ideal, y sea

$$S = \{ B \neq R \textit{ ideal de } R : A \subseteq B \}$$

$S \neq \emptyset$, ya que $A \in S$. Ordenemos a S con la inclusión. Verifiquemos que toda cadena $C = \{C_i : i \in I\}$ tiene cota superior en S, para poder aplicar Zorn.

Sea $C = \cup C_i$. Claramente $C_i \subseteq C \ \forall\, i \in I$. Veamos que $C \in S$.

Sean $a, b \in C$, entonces para algún i, $k \in I$, $a \in C_i$ y $b \in C_k$. Como C es una cadena, podemos suponer que $C_k \subseteq C_i$, así $a, b \in C_i$. Como C_i es un ideal, $a - b \in C_i$ y $ra \in C_i$, $\forall\ r \in R$.

Así $a, b \in C$ implica que $a - b \in C$ y que $ra \in C$, $\forall\, r \in R$. Luego C es un ideal.

Como $A \subseteq C_i$, $\forall\ i \in I$, entonces $A \subseteq C$. Nos falta ver que $C \neq R$. Pero como cada $C_i \neq R$, entonces $1_R \notin C_i$, $\forall i \in I$, (pues si 1_R está en algún C_i, como C_i es un ideal, entonces $C_i = R$), por lo tanto $1_R \notin C$ y así $C \neq R$. Finalmente, hemos visto que $C \in S$.

Luego el Lema de Zorn, nos dice que existe un elemento maximal en S. Pero este elemento maximal es claramente un ideal maximal en R que

contiene a A.

Recordemos que estábamos considerando un anillo conmutativo R con identidad 1_R.

Decir que $\{0\}$ es un ideal maximal en R es equivalente a decir que R es un cuerpo.

Supongamos que R es un cuerpo, y que M es un ideal maximal. Veamos que $M = \{0\}$.

Sea $m \in M$. Si $m \neq 0$, como R es un cuerpo, entonces $m^{-1} \in R$ Además, M es un ideal, por lo tanto $mr \in M$, $\forall\, r \in R$, en particular, para $r = m^{-1}$, i.e. que $1_R = mm^{-1} \in M$. Pero esto nos diría que $M = R$, pero M es maximal. Concluimos que $M = \{0\}$.

Veamos la recíproca. Supongamos ahora que $\{0\}$ es un ideal maximal. Veamos primero que R no tiene divisores de cero, i.e. si $a \in R$. $a \neq 0$ es un divisor de cero si existe $b \in R$, $b \neq 0$ tal que $ab = 0$

Supongamos que existen $a, b \neq 0$ tal que $ab = 0$. Consideremos ahora los ideales generados por a y b, que denotaremos por (a) y (b) respectivamente. (Notar que como R es conmutativo y tiene 1_R, (a)=Ra=aR). $\{0\} \subseteq (a)$ y $\{0\} \subseteq (b)$. Como $\{0\}$ es un ideal maximal, entonces $(a) = R = (b)$.

Notemos que $(a)(b) \subseteq (ab)$. Pues, sean $a_1 \in (a)$ y $b_2 \in (b)$, quiero ver que $a_1 b_2 \in (ab)$. Como $a_1 \in (a)$, entonces existe $r_1 \in R$ tal que $a_1 = ar_1$ y como $b_2 \in (b)$, entonces existe $r_2 \in R$ tal que $b_2 = br_2$, por lo tanto $a_1 b_2 = ar_1 br_2$, como R es conmutativo, $a_1 b_2 = (r_1 r_2)ab = ra_1 b_2$, lo que implica que $a_1 b_2 \in (ab)$.

Observemos también, que como $1_R \in R$, entonces $RR = R$.

Así

$$R = RR = (a)(b) \subseteq (ab) = \{0\}.$$

Absurdo que provino de suponer que R tenia divisores de cero.

Veamos ahora que si $m \in R, m \neq 0, \quad \exists \quad s \in R$ tal que $ms = 1_R$. Sea $m \neq 0$ y consideremos ahora el ideal generado por m, i.e. (m) Nuevamente, como $\{0\} \subseteq (m)$ y $\{0\}$ es un ideal maximal, entonces $(m) = R$. Como $1_R \in R = (m) = mR$, entonces existe $s \in R$ tal que $1_R = ms$.

Por lo tanto, R es un anillo de división, como además es conmutativo, entonces es un cuerpo.

Facultad de Matemática, Astronomía y Física.
Universidad Nacional de Córdoba.