Cuestiones elementales sobre Teoría de Conjuntos. Aplicaciones.

Trabajo de Fin de Grado
Facultad de Ciencias Matemáticas
Universidad Complutense de Madrid

Curso 2022-2023

Autor: Javier Lobillo Olmedo
Directores: Juan Ramón Delgado, José Francisco Fernando y José Manuel Gamboa

Madrid, a 18 de septiembre de 2023

Índice general

Agradecimientos v

Introducción vii

Extended abstract ix

I. Teorema de Cantor-Bernstein y cardinales de conjuntos de números 1
I.1. Teorema de Cantor-Bernstein 1
I.2. Cardinales de conjuntos de números 5

II. El Axioma de Elección 9
II.1. Algunos axiomas de la Teoría de Conjuntos 9
II.2. Principio de comparación de cardinales 13

III. Aplicaciones 21
III.1. Existencia y unicidad del cierre algebraico de un cuerpo 21
III.2. Existencia y equicardinalidad de las bases de un espacio vectorial 31
III.3. Existencia de ideales maximales en anillos conmutativos y unitarios . . . 34

Agradecimientos

A mi madre, y a quienes tampoco están aquí, por seguir cuidándome día a día. A mi padre, por haberme guiado en este maravilloso mundo de las matemáticas. A mis tutores, al resto de profesores del grado de Matemáticas y a Sergio, por haberme hecho mejor matemático. A mi familia y amigos, por haberme apoyado y querido.

Introducción

A lo largo de la historia, los matemáticos siempre tuvieron una intuición más o menos útil acerca de lo que son los conjuntos y cómo tratarlos. Resulta interesante, pues, que fuera tan tarde como en la década de 1870 cuando matemáticos como Georg Cantor y Richard Dedekind comenzaran a considerar la Teoría de Conjuntos como una disciplina formal y rigurosa. Una vez surgido el problema de formalizar las bases de las matemáticas, fueron muchos matemáticos los que se sumaron a dicho estudio. Entre ellos destacaron Ernst Zermelo y Abraham Fraenkel, los cuales dieron nombre en la primera mitad del siglo XX a la axiomática de conjuntos más famosa y más utilizada en la construcción formal de las matemáticas.

Sin embargo, una pregunta muy básica inquietó a la academia durante este siglo XX: ¿dado un conjunto cualquiera, puedo *tomar* un elemento suyo? Aunque resulta más natural poder establecer relaciones y proposiciones sobre elementos dados de conjuntos, no parece que siempre exista una manera clara de tomar los elementos en sí. Formalizada en 1904 por Zermelo en forma del *Axioma de elección*, esta capacidad para actuar sobre conjuntos fue planteada para demostrar su Teorema del buen orden, cuya equivalencia al primero se demuestra en este trabajo.

El Axioma de elección resultó ser sujeto de estudio por muchas personas, quienes intentaban comprender si éste se podía deducir de la Axiomática de Zermelo-Fraenkel (ZF) o si, por el contrario, resultaba ser un axioma independiente. No fue hasta 1938 cuando Kurt Gödel demostró que si ZF es consistente, entonces ZF, junto con el Axioma de elección también lo es. Por otro lado, Paul Cohen demostró en 1963 que si ZF es consistente, entonces ZF con la negación del Axioma de elección también lo es, por lo que resulta ser un axioma lógicamente independiente.

Por otra parte, Kazimierz Kuratowski y Max Zorn demostraron independientemente en 1922 y 1935 el conocido hoy en día como Lema de Zorn, suponiendo cierto el Axioma de elección. En este trabajo se presenta, además, otra formulación equivalente al Lema de Zorn y el Axioma de elección, la cual es el Principio de maximalidad de Hausdorff, introducido por él en 1914. Todas estas equivalencias se demuestran a lo largo de este trabajo, estructurado en varios capítulos y secciones.

Tras introducir nociones básicas sobre ordenación de conjuntos, dedicamos la primera sección a demostrar el Teorema de Cantor-Bernstein I.1.10, resultado que será empleado repetidas veces a lo largo de este trabajo.

En la segunda sección se prueba que $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ y $\mathbb{N} \times \mathbb{N}$ son equipotentes, mientras que

los intervalos de $\mathbb{R}$, el propio $\mathbb{R}, \mathbb{C}$ y $\mathcal{P}(\mathbb{N})$, formado por todos los subconjuntos de $\mathbb{N}$, son equipotentes entre sí, pero no con los anteriores.

El segundo capítulo constituye la parte fundamental de este trabajo. En su primera sección se demuestra que el Axioma de elección, el Lema de Zorn (y su forma débil), el Principio de buena ordenación de Zermelo y el Principio maximal de Hausdorff son equivalentes en el Teorema II.1.3.

La demostración de que el Axioma de elección implica la citada forma débil del Lema de Zorn se apoya en el denominado Lema del punto fijo de Bourbaki, II.1.5, que tiene interés por sí mismo.

En la segunda sección del segundo capítulo se responde a la siguiente pregunta: Dados dos conjuntos A y B, ¿es cierto que bien $\mathrm{Card}(A) \leq \mathrm{Card}(B)$, o bien $\mathrm{Card}(B) \leq \mathrm{Card}(A)$? Este es el llamado Principio de comparación de cardinales y la respuesta es que dicho principio es equivalente a cualquiera de los anteriormente citados.

En la Proposición II.2.1 probamos que el Lema de Zorn implica el Principio de comparación de cardinales. La prueba del recíproco requiere introducir nuevos conceptos y resultados. El más relevante es el Teorema de Hartogs, II.2.3, que afirma que, para cada conjunto no vacío A, existe un conjunto bien ordenado $(B, \leq_B)$ con cardinal estrictamente mayor.

El Lema de Zorn tiene innumerables aplicaciones a lo largo de las matemáticas. Nos hemos limitado a presentar, en el tercer capítulo, tres de ellas; eso sí, la exposición dada es esencialmente autocontenida en los tres casos. En la primera sección presentamos una demostración, debida al Prof. Z. Jelonek, de la existencia y unicidad, salvo isomorfía, del cierre algebraico de un cuerpo y que brindó a uno de los directores de este trabajo el Prof. José F. Ruiz. Hacerlo con detalle ha requerido incorporar numerosos resultados elementales sobre cardinalidad.

En la sección segunda de este capítulo se demuestra la existencia y equicardinalidad de las bases de un espacio vectorial arbitrario, mientras que en la tercera se prueba que, dados un anillo unitario y conmutativo, A, y un elemento $a \in A$ que no sea unidad, existe un ideal maximal $\mathfrak{m} \subset A$ tal que $a \in \mathfrak{m}$.

Por último, cabe hacer una breve mención a la notación utilizada en este trabajo. Los naturales, $\mathbb{N}$, incluyen al 0 y se especificará en caso contrario con la notación $\mathbb{N}_1$. La inclusión $\subset$ ha de leerse como "contenido en o igual a", mientras que los subconjuntos propios se mostrarán con $\subsetneq$. Cuando se utilice el símbolo $\bigcup$ se referirá a la unión estándar, mientras que $\bigsqcup$ se referirá a la unión disjunta. Dado un conjunto S contenido en un anillo A, se indicará al ideal generado por S como $\langle S \rangle$. Por último, $A \hookrightarrow B$ se referirá a una inyección del conjunto A en el conjunto B.

Extended abstract

After introducing basic notions of set ordering, the first section is dedicated to proving the Cantor-Bernstein Theorem, a result that will be used repeatedly throughout this work.

In the second section, it is shown that $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, and $\mathbb{N} \times \mathbb{N}$ are equipotent, while the intervals of $\mathbb{R}$, $\mathbb{R}$ itself, $\mathbb{C}$, and $\mathcal{P}(\mathbb{N})$, the power set of $\mathbb{N}$, are equipotent to each other but not to the former.

The second chapter constitutes the core part of this work. In its first section, it's demonstrated that the Axiom of Choice, Zorn's Lemma (and its weak form), Zermelo's Well-Ordering Principle, and Hausdorff's Maximality Principle are equivalent in Theorem II.1.3.

The proof that the Axiom of Choice implies the aforementioned weak form of Zorn's Lemma relies on the so-called Bourbaki Fixed Point Lemma, II.1.5, which is of interest on its own.

In the second section of the second chapter, the following question is answered: Given two sets A and B, is it true that either $\mathrm{Card}(A) \leq \mathrm{Card}(B)$, or $\mathrm{Card}(B) \leq \mathrm{Card}(A)$? This is the so-called Cardinal Comparison Principle, and the answer is that this principle is equivalent to any of the previously mentioned principles.

In Proposition II.2.1, we prove that Zorn's Lemma implies the Cardinal Comparison Principle. The proof of the converse requires introducing new concepts and results. The most relevant is Hartogs' Theorem, II.2.3, which asserts that, for every non-empty set A, there exists a well-ordered set $(B, \leq_B)$ with strictly greater cardinality.

Zorn's Lemma has countless applications throughout mathematics. We have limited ourselves to presenting three of them in the third chapter; however, the presentation given is essentially self-contained in all three cases. In the first section, we present a proof, due to Prof. Z. Jelonek, of the existence and uniqueness, up to isomorphism, of the algebraic closure of a field, a result provided by one of the supervisors of this work, Prof. José F. Ruiz. Doing so in detail required incorporating numerous elementary results about cardinality.

In the second section of this chapter, the existence and equicardinality of bases for an arbitrary vector space are demonstrated, while in the third section, it is proven that, given a commutative unitary ring A and an element $a \in A$ that is not a unit, there exists a maximal ideal $\mathfrak{m} \subset A$ such that $a \in \mathfrak{m}$.

Finally, a brief note is made about the notation used in this work. The natural numbers, $\mathbb{N}$, include 0, and it will be specified otherwise with the notation $\mathbb{N}_1$. The inclusion $\subset$

should be read as ïs contained in or equal to,"while proper subsets will be indicated with $\subsetneq$. When the symbol $\bigcup$ is used, it refers to the standard union, while $\bigsqcup$ refers to the disjoint union. Given a set S contained in a ring A, the ideal generated by S will be denoted as $\langle S \rangle$. Finally, $A \hookrightarrow B$ will refer to an injection of the set A into the set B.

Capítulo I

Teorema de Cantor-Bernstein y cardinales de conjuntos de números

I.1. Teorema de Cantor-Bernstein

Definición I.1.1. Sean $(A, \leq)$ un conjunto parcialmente ordenado y $B \subset A$ un subconjunto.

(1) Se dice que un elemento $b \in B$ es el *mínimo* de B y se escribe $b := \min(B)$ si $b \leq x$ para todo $x \in B$.

(2) Se dice que $\leq$ es un *buen orden*, o que $(A, \leq)$ está *bien ordenado*, si todo subconjunto de A tiene un mínimo.

(3) Un elemento $a \in A$ se dice una *cota superior* de B si $x \leq a$ para todo $x \in B$.

(4) Se dice que un elemento $a \in A$ es *supremo* de B, y se escribe $a := \sup(B)$, si a es cota superior de B y $a \leq x$ para toda cota superior $x \in A$ de B.

(5) Un elemento $a \in A$ se dice *maximal* si no existe $x \in A$ tal que $a < x$.

Definición I.1.2. Dados dos conjuntos A y B se dice que el *cardinal* de A es *menor o igual* que el cardinal de B, y se escribe $\mathrm{Card}(A) \leq \mathrm{Card}(B)$, si existe una aplicación inyectiva $F : A \to B$.

Si F se puede encontrar biyectiva entonces decimos que A y B *tienen el mismo cardinal* o que A y B son *equipotentes* y escribimos $\mathrm{Card}(A) = \mathrm{Card}(B)$. Si no existe tal biyección escribimos $\mathrm{Card}(A) \neq \mathrm{Card}(B)$.

Si $\mathrm{Card}(A) \leq \mathrm{Card}(B)$ pero $\mathrm{Card}(A) \neq \mathrm{Card}(B)$ se dice que el cardinal de A es *(estrictamente) menor que* el cardinal de B y se escribe $\mathrm{Card}(A) < \mathrm{Card}(B)$.

Proposición I.1.3. *La propiedad entre dos conjuntos dada por* ser equipotentes *es reflexiva, simétrica y transitiva.*

Demostración. Como la identidad es biyectiva, entonces $\mathrm{Card}(A) = \mathrm{Card}(A)$ para todo conjunto A. Además, es simétrica, pues la aplicación inversa de una aplicación biyectiva es también biyectiva. Por último, si $\mathrm{Card}(A) = \mathrm{Card}(B)$ y $\mathrm{Card}(B) = \mathrm{Card}(C)$, existen $F : A \to B$ y $G : B \to C$ ambas biyectivas, por lo que la composición $G \circ F : A \to C$ es también una biyección y $\mathrm{Card}(A) = \mathrm{Card}(C)$. □

Informalmente, podríamos leer la observación como que la propiedad "ser equipotentes" es una relación de equivalencia. Sin embargo esto no es posible formalmente ya que una relación (de equivalencia) se define sobre un conjunto y no existe el conjunto que contiene a todos los conjuntos, según los *Axiomas de Zermelo-Fraenkel*.

Proposición I.1.4. *La propiedad definida entre dos conjuntos dada por* tener cardinal menor o igual *es reflexiva y transitiva.*

Demostración. En efecto, como hemos mostrado en la observación anterior, para todo conjunto A se cumple $\mathrm{Card}(A) = \mathrm{Card}(A)$ y, como toda aplicación biyectiva es a su vez inyectiva, $\mathrm{Card}(A) \leq \mathrm{Card}(A)$. Por otro lado, sean A, B y C tres conjuntos tales que $\mathrm{Card}(A) \leq \mathrm{Card}(B) \leq \mathrm{Card}(C)$. Entonces existen aplicaciones inyectivas $F : A \to B$ y $G : B \to C$. Como la composición de aplicaciones inyectivas es inyectiva, tenemos que $G \circ F : A \to C$ es inyectiva y $\mathrm{Card}(A) \leq \mathrm{Card}(C)$. □

Observación I.1.5. Si $A \subset B$ entonces $\mathrm{Card}(A) \leq \mathrm{Card}(B)$ ya que la aplicación inclusión $j : A \hookrightarrow B$ es inyectiva.

Definición I.1.6. (1) Un conjunto A se dice *finito* si, o bien es vacío, o bien es equipotente al conjunto $I_n := \{k \in \mathbb{N} : 1 \leq k \leq n\}$ para algún número natural $n \geq 1$. En el primer caso se dice que $\mathrm{Card}(A) = 0$ y, en el segundo, que $\mathrm{Card}(A) = n$.

(2) Un conjunto A se dice *infinito* si existe $a \in A$ tal que los conjuntos A y $A \setminus \{a\}$ son equipotentes.

Por ejemplo, vemos que el conjunto $\mathbb{N}$ de los números naturales es infinito, pues la aplicación *sucesor* $s : \mathbb{N} \to \mathbb{N} \setminus \{0\}, n \mapsto n+1$ es biyectiva. Se suele denotar $\mathrm{Card}(\mathbb{N}) := \aleph_0$.

Lema I.1.7. *Sean A y B dos conjuntos biyectivos. Entonces A es infinito si y sólo si B es infinito.*

Demostración. Si A es infinito, sea $a \in A$ tal que A y $C := A \setminus \{a\}$ son equipotentes, es decir, existe una biyección $F : A \to C$. Como A y B son equipotentes, existe una biyección $G : A \to B$. Sea $b = G(a)$, entonces tenemos que $G|_C : C \to B \setminus \{b\}$ es una biyección. Por tanto tenemos que la composición $H = G|_C \circ F \circ G^{-1} : B \to B \setminus \{b\}$ es una biyección y B es infinito. □

Proposición I.1.8. *Los conjuntos finitos no son infinitos.*

Demostración. Como el conjunto vacío no tiene subconjuntos propios, no es infinito.

Supongamos que existe un conjunto no vacío finito e infinito. Consideramos los conjuntos I_n que son equipotentes con dicho conjunto finito e infinito. Al ser $\mathbb{N}$ bien ordenado, podemos tomar el $n \in \mathbb{N}$ mínimo para el cual existe un I_n que cumple esta propiedad. Por el lema anterior, nos vale demostrar que I_n no es infinito.

En efecto, si lo fuese, existirían $k \in I_n$ y una biyección $F : I_n \to I_n \setminus \{k\}$. Si $k = n$ tenemos que I_n e I_{n-1} son equipotentes y, por el lema anterior, I_{n-1} sería también infinito, contradiciendo la minimalidad de n.

En caso contrario, consideramos la biyección

$$G : I_n \setminus \{k\} \to I_{n-1}, m \mapsto \begin{cases} k & \text{si } m = n, \\ m & \text{si } m \neq n. \end{cases}$$

Por tanto, la composición $H = G \circ F : I_n \to I_{n-1}$ es una biyección, por lo que llegamos a la misma contradicción. □

En el tercer capítulo demostraremos que los conjuntos no finitos son, en efecto, infinitos.

Proposición I.1.9. *Para cada conjunto A finito o infinito se cumple que* $\mathrm{Card}(A) < \mathrm{Card}(\mathcal{P}(A))$.

Demostración. Si A es finito y $\mathrm{Card}(A) = n$, el conjunto A tiene $\binom{n}{k}$ subconjuntos con k elementos para cada $k = 0, \ldots, n$. Por tanto, el conjunto $\mathcal{P}(A)$ tiene

$$\sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n$$

elementos. Por tanto, $\mathrm{Card}(A) = n < 2^n = \mathrm{Card}(\mathcal{P}(A))$.

Supongamos entonces que A es infinito. Desde luego $\mathrm{Card}(A) \leq \mathrm{Card}(\mathcal{P}(A))$, ya que la aplicación $A \to \mathcal{P}(A), x \mapsto \{x\}$ es inyectiva.

Si existiese una biyección $F : A \to \mathcal{P}(A)$, sea $M := \{x \in A : x \notin F(x)\}$, posiblemente vacío. Por ser F sobreyectiva existe $a \in A$ tal que $M = F(a)$ y puede suceder que $a \in M$ o $a \notin M$. En el primer caso $a \notin F(a) = M$, mientras que en el segundo $a \in F(a) = M$. En ambos casos se da una contradicción, luego $\mathrm{Card}(A) \neq \mathrm{Card}(\mathcal{P}(A))$, por lo que $\mathrm{Card}(A) < \mathrm{Card}(\mathcal{P}(A))$. □

Teorema I.1.10 (Teorema de Cantor-Bernstein). *Sean A y B dos conjuntos tales que* $\mathrm{Card}(A) \leq \mathrm{Card}(B)$ *y* $\mathrm{Card}(B) \leq \mathrm{Card}(A)$. *Entonces* $\mathrm{Card}(A) = \mathrm{Card}(B)$.

Demostración. Hay que demostrar que si existen aplicaciones inyectivas $F : A \to B$ y $G : B \to A$ entonces existe una biyección entre A y B. Consideremos la aplicación

$$\Phi : \mathcal{P}(A) \to \mathcal{P}(A), M \mapsto A \setminus G(B \setminus F(M)),$$

que respeta inclusiones, esto es, si $M \subset N \subset A$, entonces $\Phi(M) \subset \Phi(N) \subset A$. En efecto, como $F(M) \subset F(N)$, entonces $B \setminus F(N) \subset B \setminus F(M)$, luego

$$G(B \setminus F(N)) \subset G(B \setminus F(M))$$

y, tomando complementarios de nuevo,

$$\Phi(M) = A \setminus G(B \setminus F(M)) \subset A \setminus G(B \setminus F(N)) = \Phi(N).$$

Consideramos la familia de subconjuntos $\Sigma := \{M \in \mathcal{P}(A) : M \subset \Phi(M)\}$ que es no vacía ya que contiene al conjunto vacío. Consideramos la unión de sus miembros $X := \bigcup_{M\in\Sigma} M$ y vemos que tiene la propiedad de que coincide con su imagen por Φ, esto es, $\Phi(X) = X$. En efecto, cada $M \in \Sigma$ está contenido en $\Phi(M)$, luego

$$X = \bigcup_{M\in\Sigma} M \subset \bigcup_{M\in\Sigma} \Phi(M) = \Phi(\bigcup_{M\in\Sigma} M) = \Phi(X). \tag{I.1}$$

Para probar la inclusión $\Phi(X) \subset X$ nótese que, haciendo actuar Φ sobre ambos miembros de (I.1), se tiene que $\Phi(X) \subset \Phi(\Phi(X))$, luego $\Phi(X) \in \Sigma$, por lo que $\Phi(X) \subset \bigcup_{M\in\Sigma} M = X$ y hemos probado que $X = \Phi(X)$.

El conjunto X cumple que $A \setminus X \subset G(B)$. En efecto, como Φ preserva inclusiones, tenemos

$$A \setminus G(B) = A \setminus G(B \setminus F(\varnothing)) = \Phi(\varnothing) \subset \Phi(A \setminus G(B)),$$

es decir, $A \setminus G(B) \in \Sigma$, luego $A \setminus G(B) \subset X$ o, lo que es lo mismo, $A \setminus X \subset G(B)$. Por esto, además de la inyectividad de G, resulta bien definida la aplicación

$$H : A \to B, x \mapsto \begin{cases} F(x) & \text{si } x \in X, \\ G^{-1}(x) & \text{si } x \in A \setminus X, \end{cases}$$

que es la biyección buscada. Para comprobarlo, observamos en primer lugar que

$$A \setminus X = A \setminus \Phi(X) = G(B \setminus F(X)),$$

es decir,

$$B \setminus F(X) = G^{-1}(A \setminus X) = H(A \setminus X). \tag{I.2}$$

Para ver que H es inyectiva, comprobamos que, al serlo F, si $x, y \in X$, con $x \neq y$, entonces $F(x) \neq F(y)$, es decir, $H(x) \neq H(y)$. Por otro lado, si tomamos $x, y \in A \setminus X$ distintos, entonces, por ser G^{-1} una aplicación inversa, tenemos también que $H(x) \neq H(y)$. Por tanto, queda comprobar que si tomamos $x \in X$ e $y \in A \setminus X$, entonces $H(x) \neq H(y)$. Pero esto es evidente si observamos que $H(x) = F(x) \in F(X)$, mientras que se desprende de (I.2) que $H(y) \in B \setminus F(X)$.

Observamos que, de nuevo por (I.2), tenemos

$$im(H) = H(X) \cup H(A \setminus X) = F(X) \cup G^{-1}(A \setminus X) = F(X) \cup B \setminus F(X) = B,$$

por lo que se deduce la sobreyectividad de H. □

I.2. Cardinales de conjuntos de números

Proposición I.2.1. *(1) Los conjuntos $\mathbb{N}$, $\mathbb{Z}$ y $\mathbb{Q}$ de los números naturales, enteros y racionales, respectivamente, son equipotentes.*

(2) Cada intervalo con más de un punto de los números reales, denotados $\mathbb{R}$, tiene el mismo cardinal que el propio $\mathbb{R}$ que, a su vez, se suele denotar como $\mathrm{Card}(\mathbb{R}) := \aleph_1$.

(3) Los números complejos, denotados $\mathbb{C}$, son equipotentes con $\mathbb{R}$.

(4) Si A, B denotan dos conjuntos equipotentes, entonces $\mathrm{Card}(\mathcal{P}(A)) = \mathrm{Card}(\mathcal{P}(B))$.

(5) El conjunto $\mathcal{P}(\mathbb{N})$ formado por todos los subconjuntos de $\mathbb{N}$ es equipotente con $\mathbb{R}$.

(6) El producto cartesiano $\mathbb{N} \times \mathbb{N}$ es equipotente con $\mathbb{N}$.

Demostración. (1) Puesto que $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$ todo se reduce, a la vista del Teorema de Cantor-Bernstein I.1.10 a encontrar una aplicación inyectiva $\mathbb{Q} \to \mathbb{N}$ que demuestre $Card(\mathbb{Q}) \leq Card(\mathbb{N})$. Observamos que cada $x \in \mathbb{Q} \setminus \{0\}$ se escribe, de modo único, de la forma $x = \frac{\varepsilon m}{n}$, donde $\varepsilon = \pm 1$ y $m, n \in \mathbb{N}$ son coprimos. Por el Teorema Fundamental de la Aritmética, la aplicación

$$F : \mathbb{Q} \to \mathbb{N}, x := \frac{\varepsilon m}{n} \mapsto \begin{cases} 0 & \text{si } x = 0, \\ 2^m \cdot 3^n & \text{si } \varepsilon = 1, \\ 2^m \cdot 3^n \cdot 5 & \text{si } \varepsilon = -1, \end{cases}$$

es, en efecto, inyectiva.

(2) Observamos en primer lugar que si $a < b$ son números reales, entonces el intervalo abierto (a, b) es equipotente con $(0, 1)$ vía la biyección

$$(0, 1) \to (a, b), t \mapsto (1 - t)a + tb.$$

En particular, tenemos que $\mathrm{Card}((0, 1)) = \mathrm{Card}((a, b)) = \mathrm{Card}((-1, 1))$.

Sea entonces $I \subset \mathbb{R}$ un intervalo cualquiera. Eligiendo dos puntos $a < b \in I$ cualesquiera, como $(a, b) \subset I \subset \mathbb{R}$, tenemos que

$$\mathrm{Card}((-1, 1)) = \mathrm{Card}(a, b) \leq \mathrm{Card}(I) \leq \mathrm{Card}(\mathbb{R})$$

luego, por el Teorema de Cantor-Bernstein, basta encontrar una inyección de $\mathbb{R}$ en $(-1, 1)$. Se comprueba inmediatamente que la aplicación

$$F : \mathbb{R} \to (-1, 1), t \mapsto \frac{t}{1 + |t|}$$

es inyectiva, luego hemos terminado.

(3) Por el apartado anterior, tenemos que existe una biyección $G : \mathbb{R} \to [0,1]$, la cual induce a su vez otra biyección

$$H : \mathbb{C} \to [0,1] \times [0,1], x + iy \mapsto (G(x), G(y)).$$

Por otro lado vemos que la aplicación $\varphi : [0,1] \times [0,1] \to [0,1]$ definida por

$$\varphi\left(\sum_{k\in\mathbb{N}\setminus\{0\}} u_k 10^{-k}, \sum_{k\in\mathbb{N}\setminus\{0\}} v_k 10^{-k}\right) = \sum_{k\in\mathbb{N}\setminus\{0\}} u_k 10^{-(2k-1)} + \sum_{k\in\mathbb{N}\setminus\{0\}} v_k 10^{-2k},$$

donde $0 \leq u_k, v_k \leq 9$, es también biyección, luego la composición $G^{-1} \circ \varphi \circ H : \mathbb{C} \to \mathbb{R}$ es biyectiva y concluimos $\mathrm{Card}(\mathbb{C}) = \mathrm{Card}(\mathbb{R})$.

(4) Sea $f : A \to B$ una biyección. Hemos de demostrar que $\widehat{f} : \mathcal{P}(A) \to \mathcal{P}(B)$, definida como $\widehat{f}(A') := f(A')$ para $A' \subset A$, es una biyección.

Vemos que es inyectiva pues, si $\widehat{f}(A') = \widehat{f}(A'')$, entonces $f(A') = f(A'')$, luego

$$A' = f^{-1}(f(A')) = f^{-1}(f(A'')) = A''.$$

Para terminar, vemos que $\widehat{f}$ es sobreyectiva. En efecto, dado un subconjunto $B' \subset B$, por ser f biyección, existe un subconjunto $A' := f^{-1}(B') \subset A$ que cumple

$$\widehat{f}(A') = f(f^{-1}(B)) = B$$

y hemos acabado.

(5) En el apartado (2) hemos demostrado que $\mathbb{R}$ e $I = [0,1)$ son equipotentes. Además, $\mathbb{N}_1 := \mathbb{N} \setminus \{0\}$ y $\mathbb{N}$ lo son como hemos visto después de I.1.6, luego $\mathrm{Card}(\mathcal{P}(\mathbb{N}_1)) = \mathrm{Card}(\mathcal{P}(\mathbb{N}))$ por el apartado anterior. Basta, por tanto, construir aplicaciones inyectivas $F : \mathcal{P}(\mathbb{N}_1) \to I$ y $G : I \to \mathcal{P}(\mathbb{N}_1)$.

Sea

$$F : \mathcal{P}(\mathbb{N}_1) \to I, X \mapsto \sum_{n\in X} \frac{1}{3^n}.$$

Si X e Y son subconjuntos distintos de $\mathbb{N}_1$, la diferencia simétrica $Z = (X \setminus Y) \cup (Y \setminus X)$ es no vacío, luego existe $m := \mathrm{mín}(Z)$ por ser $\mathbb{N}$ bien ordenado. Podemos suponer que $m \in X \setminus Y$, y resulta

$$F(X) - F(Y) = \frac{1}{3^m} + \sum_{\substack{n\in X\setminus Y \\ n>m}} \frac{1}{3^n} - \sum_{n\in Y\setminus X} \frac{1}{3^n} + \sum_{n\in X\cup Y} \frac{1}{3^n} - \sum_{n\in Y\cup X} \frac{1}{3^n} \geq$$

$$\frac{1}{3^m} - \sum_{n\geq m+1} \frac{1}{3^n} = \frac{1}{3^m} - \frac{1}{3^{m+1}} \cdot \frac{1}{1-1/3} = \frac{1}{3^m} - \frac{1}{2\cdot 3^m} > 0.$$

luego $F(X) \neq F(Y)$ y F es inyectiva. Por otro lado, es evidente la inyectividad de

$$G : I \to \mathcal{P}(\mathbb{N}_1), u := \sum_{n\in\mathbb{N}_1} u_n 2^{-n} \mapsto \{n \in \mathbb{N}_1 : u_n = 1\}, \text{ donde } u_n \in \{0, 1\}.$$

(6) Las aplicaciones

$$F : \mathbb{N} \to \mathbb{N}_1, n \mapsto n + 1 \text{ y } G : \mathbb{N} \times \mathbb{N} \to \mathbb{N}_1 \times \mathbb{N}_1, (m, n) \mapsto (m + 1, n + 1)$$

son biyectivas, luego basta probar que $\mathbb{N}_1$ y $\mathbb{N}_1 \times \mathbb{N}_1$ son equipotentes. Esto se deduce del Teorema de Cantor-Bernstein, I.1.10, pues las aplicaciones

$$\varphi : \mathbb{N}_1 \to \mathbb{N}_1 \times \mathbb{N}_1, n \mapsto (n, 1) \quad \text{y} \quad \phi : \mathbb{N}_1 \times \mathbb{N}_1 \to \mathbb{N}_1, (n, m) \mapsto 2^n \cdot 3^m$$

son claramente inyectivas.

□

Observación I.2.2. (1) Se desprende de I.2.1 (3) que el plano y la recta real son equipotentes. Este resultado debido a Cantor es el que él mismo pretendía refutar y para lo que desarrolló la Teoría de Cardinales. Años después se introdujo el concepto de homeomorfismo, que permite distinguir entre ambos entes: aunque existen aplicaciones biyectivas y continuas de la recta en el plano, ninguna tiene inversa continua.

(2) Se deduce de I.1.9 y I.2.1 (5) que $\mathrm{Card}(\mathbb{N}) < \mathrm{Card}(\mathcal{P}(\mathbb{N})) = \mathrm{Card}(\mathbb{R})$, lo que además pone de manifiesto que existen conjuntos infinitos no equipotentes. La llamada *Hipótesis del Continuo* afirma que no existe ningún conjunto S tal que $\mathrm{Card}(\mathbb{N}) < \mathrm{Card}(S) < \mathrm{Card}(\mathbb{R})$, y el primero de los problemas que planteó Hilbert en su conferencia de París del año 1900 consistía en demostrar o refutar esta hipótesis. En 1940 Gödel demostró que si la Teoría de Conjuntos es consistente, también es consistente la Teoría de Conjuntos junto con la Hipótesis del Continuo. En 1963 Cohen demostró que si la Teoría de Conjuntos es consistente, también lo es junto con la negación de la hipótesis del continuo. Estos dos hechos se expresan diciendo que la Hipótesis del Continuo es *indecidible* en la Teoría de Conjuntos.

(3) Hemos demostrado en el apartado 2 de la Proposición I.2.1, usando el Teorema de Cantor-Bernstein, que todos los intervalos tienen el mismo cardinal, pero queremos presentar la biyección entre los intervalos $(0, 1]$ y $(0, 1)$ que el Prof. Javier Gallego Rodrigo mostró siendo alumno del primer curso de la antigua Licenciatura en Matemáticas. Denotamos $x_n := 1/n$ para cada $n \in \mathbb{N}_1$ y $S := \{x_n : n \in \mathbb{N}_1\}$. La biyección encontrada por Gallego es

$$f : (0, 1] \to (0, 1), x \mapsto \begin{cases} x_{n+1} & \text{si } x = x_n, \\ x & \text{si } x \in (0, 1] \setminus S. \end{cases}$$

Capítulo II

El Axioma de Elección

II.1. Algunos axiomas de la Teoría de Conjuntos

Definición II.1.1. Sea $(A, \leq)$ un conjunto parcialmente ordenado.

(1) Una *cadena* en $(A, \leq)$ es un subconjunto no vacío $C \subset A$ que, con la restricción del orden de A, está totalmente ordenado.

(2) Se dice que $(A, \leq)$ es *inductivo* si toda cadena C de A está acotada superiormente, es decir, $\exists x \in A$ tal que $y \leq x, \forall y \in C$.

(3) Se dice que $(A, \leq)$ es *totalmente inductivo* si toda cadena $C \subset A$ tiene supremo.

En este capítulo se probará la equivalencia de los axiomas introducidos a continuación.

Definición II.1.2. (1) *Axioma de Elección.* Para cada conjunto no vacío A existe una aplicación $F : \mathcal{P}(A) \setminus \varnothing \to A$ tal que $F(M) \in M, \forall M \in \mathcal{P}(A) \setminus \varnothing$.

(2) *Lema de Zorn.* Todo conjunto no vacío parcialmente ordenado inductivo tiene algún elemento maximal.

(3) *Principio de la buena ordenación de Zermelo.* Para cada conjunto A existe una relación de orden $\leq$ en A tal que $(A, \leq)$ está bien ordenado.

(4) *Forma débil del Lema de Zorn.* Todo conjunto no vacío parcialmente ordenado totalmente inductivo tiene algún elemento maximal.

(5) *Principio maximal de Hausdorff.* Todo conjunto parcialmente ordenado $(A, \leq)$ tiene un subconjunto totalmente ordenado que es maximal entre los subconjuntos totalmente ordenados de $(A, \leq)$.

El objetivo de este capítulo es demostrar el siguiente teorema.

Teorema II.1.3. *Los siguientes enunciados son equivalentes:*

1. *El Axioma de elección.*
2. *La forma débil del Lema de Zorn.*
3. *El Principio maximal de Hausdorff.*
4. *El Lema de Zorn.*
5. *El Principio de la buena ordenación de Zermelo.*

En la demostración de que el Axioma de elección implica la forma débil del Lema de Zorn utilizaremos la siguiente definición y el lema posterior debido a Bourbaki.

Definición II.1.4. Sean $(A, \leq)$ un conjunto no vacío totalmente inductivo, un punto $a \in A$ y $f : A \to A$ una aplicación. Se dice que un subconjunto $X \subset A$ es *saturado* (respecto a a) si $a \in X$, $f(X) \subset X$ y para cada $Y \subset X$ totalmente ordenado se cumple que $\sup(Y) \in X$.

Lema II.1.5 (Lema del punto fijo de Bourbaki)**.** *Sean $(A, \leq)$ un conjunto no vacío totalmente inductivo y $f : A \to A$ una aplicación tal que $x \leq f(x)$ para cada $x \in A$. Entonces existe $z \in A$ tal que $f(z) = z$.*

Demostración. Fijamos un elemento $a \in A$ y vemos que el conjunto $Z := \{x \in A : a \leq x\}$ es saturado. En efecto, $a \in Z$, para cada $x \in Z$ se cumple $a \leq x \leq f(x)$, es decir, $f(Z) \subset Z$ y, dado $Y \subset Z$, todos los elementos de Y son mayores o iguales que a, por lo que $\sup(Y) \geq a$ y $\sup(Y) \in Z$. En consecuencia, la familia Σ formada por todos los subconjuntos saturados de A es no vacía y definimos $M := \bigcap_{X \in \Sigma} X$. Veamos que es saturado, lo que implica que es el menor subconjunto saturado de A. En efecto, $a \in X$ para cada $X \in \Sigma$, luego $a \in M$. Además, $f(X) \subset X$ para cada $X \in \Sigma$ y por tanto,

$$f(M) = f(\bigcap_{X \in \Sigma} X) \subset \bigcap_{X \in \Sigma} f(X) \subset \bigcap_{X \in \Sigma} X = M.$$

Por último, dados $Y \subset M$ y $X \in \Sigma$ se cumple que $Y \subset X$ y, como X es saturado, también $\sup(Y) \in X$, es decir, $\sup(Y) \in \bigcap_{X \in \Sigma} X = M$.

Nuestro objetivo será demostrar que M es un subconjunto totalmente ordenado. Asumamos esto por un momento. Entonces, como $(A, \leq)$ es totalmente inductivo, existe $z = \sup(M) \in M$ y este elemento cumple que $f(z) = z$. En efecto, como M es saturado, $f(z) \in f(M) \subset M$, por lo que $f(z) \leq \sup(M) = z$. Por otro lado, la desigualdad $z \leq f(z)$ la cumplen todos los elementos de A, luego $f(z) = z$.

Así pues basta probar que M está totalmente ordenado. Para ello introducimos la noción de punto extremo de M. Diremos que un elemento $e \in M$ es un *extremo* de M si todo $x \in M$ que cumple $x < e$ satisface la desigualdad $f(x) \leq e$ y denotamos $E := \{e \in M : e \text{ es extremo de } M\}$. Para cada $e \in E$ definimos el conjunto

$$M_e := \{x \in M : x \leq e \text{ o } f(e) \leq x\},$$

y vamos a comprobar que es saturado.

En primer lugar, $e \in E \subset M \subset Z$, luego $a \leq e$, lo que implica que $a \in M_e$. Además, hemos de probar que para todo $x \in M_e$ también $f(x) \in M_e$. Puede suceder una de estas dos cosas: bien $x \leq e$, bien $f(e) \leq x$.

- Si $x \leq e$ podemos distinguir dos subcasos:
  - Si $x < e$ entonces, por ser e extremo de M, se cumple que $f(x) \leq e$ y, por tanto, $f(x) \in M_e$.
  - Si $x = e$ entonces $f(e) = f(x) \leq f(x)$, lo que también implica que $f(x) \in M_e$.
- Si $f(e) \leq x \leq f(x)$, tememos que $f(e) \leq f(x)$ y así $f(x) \in M_e$.

Por último, dado un subconjunto totalmente ordenado $Y \subset M_e$ o bien cada elemento $x \in Y$ cumple $x \leq e$ o bien existe $y \in Y$ con $y \nleq e$. En el primer caso $\sup(Y) \leq e$ y $\sup(Y) \in M_e$ por ser e cota superior de Y. En el segundo caso, $y \in Y \subset M_e$ e y no es menor o igual que e, lo que implica que $f(e) \leq y \leq \sup(Y)$, de donde $\sup(Y) \in M_e$.

Hemos probado que M_e es saturado, por lo que $M \subset M_e \subset M$, o sea, $M = M_e$ para cada $e \in E$. Por tanto, dados $x \in M$ y $e \in E$ se cumple que bien $x \leq e$ o bien $f(e) \leq x$.

Vamos a demostrar ahora que el conjunto E es también saturado, lo que implica que $E = M$. En primer lugar $a \in E$ trivialmente pues no existe ningún $x \in M$ menor que a ya que cada $x \in M \subset Z$, luego $a \leq x$. A continuación probamos que $f(E) \subset E$. Supongamos lo contrario y sea $e \in E$ tal que $f(e) \notin E$. Esto significa que existe $x \in M$ tal que $x < f(e)$ pero $f(x) \nleq f(e)$ (si no existiera tal punto, $f(e)$ sería trivialmente extremo). Ahora bien, $x \in M = M_e$, por lo que bien $x < e$, bien $x = e$ o bien $f(e) \leq x$. Lo segundo implica $f(x) = f(e)$, que es falso, y lo último es imposible porque $x < f(e)$. En consecuencia $x < e$, lo que implica, por ser e un extremo de M, que $f(x) \leq e \leq f(e)$ y esto es una contradicción.

Para concluir que E es saturado, sea $Y \subset E$ una cadena y hemos de probar que $\sup(Y) \in E$. Sea por tanto $x \in M$ tal que $x < \sup(Y)$ y debemos demostrar que $f(x) \leq \sup(Y)$. Obsérvese que cada $y \in Y$ cumple que $y \in E$, luego $M = M_y$ y, en particular, $x \in M_y$. Por tanto, bien $x \leq y$ o bien $f(y) \leq x$. Si sucediese esto último para todo $y \in Y$, entonces $y \leq f(y) \leq x, \forall y \in Y$ por lo que $\sup(Y) \leq x$, lo que es falso. Por tanto, existe $y_0 \in Y$ tal que $x \leq y_0$ y distinguimos según $x < y_0$ o $x = y_0$. En el primer caso $x < y_0 \in E$, lo que significa que $f(x) \leq y_0 \leq \sup(Y)$, como queremos. En el segundo, $x = y_0 \in E$, lo que implica que $M = M_x$. Como $Y \subset E \subset M$ y M es saturado, $\sup(Y) \in M = M_x$, así que, o bien $\sup(Y) \leq x$ o bien $f(x) \leq \sup(Y)$. Lo primero es falso, porque $x < \sup(Y)$, así que $f(x) \leq \sup(Y)$ como queríamos demostrar.

Hemos probado, por tanto, que $E = M$, lo que implica que M es un subconjunto totalmente ordenado y ya señalamos que esto termina la demostración. En efecto, dados $x, y \in M$ se tiene $x \in M$ e $y \in E$, por lo que $x \in M = M_y$ así que , o bien $x \leq y$, o bien $y \leq f(y) \leq x$. □

Demostración de II.1.3. (1) $\implies$ (2) Sea $(A, \leq)$ un conjunto parcialmente ordenado y totalmente inductivo. Por hipótesis, existe una aplicación $\varphi : \mathcal{P}(A) \setminus \{\varnothing\} \to A$ tal que $\varphi(X) \in X$ para cada subconjunto no vacío $X \subset A$. Para cada elemento $x \in A$ denotamos $A_x := \{y \in A : x < y\}$ y definimos

$$f : A \to A, x \mapsto \begin{cases} x & \text{si } x \text{ es elemento maximal de } A, \\ \varphi(A_x) & \text{si } x \text{ no es elemento maximal de } A. \end{cases}$$

Para cada $x \in A$ no maximal se cumple que $f(x) \in A_x$, luego $x < f(x)$. Por tanto $x \leq f(x)$ para cada $x \in A$ y, por el Lema del punto fijo de Bourbaki II.1.5 existe $z \in A$ tal que $f(z) = z$, lo que sólo ocurre si z es un elemento maximal de A.

(2) $\implies$ (3) Sea $(A, \leq)$ un conjunto parcialmente ordenado y denotemos

$$T_A := \{X \subset A : X \text{ es totalmente ordenado}\}.$$

Vamos a demostrar que $(T_A, \subset)$ es un conjunto parcialmente ordenado, no vacío y totalmente inductivo. Evidentemente es no vacío si $A \neq \varnothing$, pues los subconjuntos formados por un único punto son totalmente ordenados. La ordenación parcial inducida por $\subset$ también es evidente.

Para ver que es totalmente inductivo, tomemos Σ un subconjunto totalmente ordenado de T_A y comprobemos que $S := \bigcup_{X \in \Sigma} X$ pertenece a T_A y es el supremo de Σ. Primero veamos que S es un subconjunto de A totalmente ordenado. Dados $x, y \in S$, existen $X, Y \in \Sigma$ tales que $x \in X$ e $y \in Y$. Puesto que Σ está totalmente ordenado, o bien $X \subset Y$, en cuyo caso $x, y \in Y$, o bien $Y \subset X$, lo que implica $x, y \in X$. En cualquier caso x, y son elementos de un subconjunto totalmente ordenado de A, por lo que o bien $x \leq y$ o bien $y \leq x$, lo que demuestra que S es totalmente ordenado.

Hemos demostrado que $S \in T_A$, por lo que nos queda comprobar que $S = \sup(\Sigma)$. Desde luego cada $X \in \Sigma$ está contenido en S. Además, si R es una cota superior de Σ, entonces contiene a todos los conjuntos que pertenecen a Σ, luego también a su unión, es decir, $S \subset R$.

Como la hipótesis dice que se cumple la forma débil del Lema de Zorn, el conjunto parcialmente ordenado y totalmente inductivo $(T_A, \subset)$ tiene algún elemento maximal, es decir, A posee un subconjunto totalmente ordenado maximal.

(3) $\implies$ (4) Sea $(A, \leq)$ un conjunto parcialmente ordenado inductivo. Por el Principio maximal de Hausdorff existe un subconjunto totalmente ordenado X de A maximal. Como $(A, \leq)$ es un conjunto inductivo y X es totalmente ordenado, existe $x \in A$ que es cota superior de X. Vamos a demostrar que x es un elemento maximal de A. Si suponemos lo contrario, entonces existe $y \in A$ tal que $x < y$. El conjunto $Y := X \cup \{y\}$ es totalmente ordenado y contiene a X, luego ambos coinciden. En particular $y \in X$ y, por ser x cota superior de X, necesariamente $y \leq x$, que es una contradicción.

(4) $\implies$ (5) Sea A un conjunto no vacío. Definimos el conjunto

$$\Sigma := \{(B, \leq_B) : B \subset A \text{ y } (B, \leq_B) \text{ está bien ordenado}\}$$

y se trata de demostrar que existe un orden $\leq_A$ en A tal que $(A, \leq_A) \in \Sigma$.

Consideramos en Σ la siguiente relación de orden: $(B, \leq_B) \leq (C, \leq_C)$ si $B \subset C$, el orden $\leq_B$ es la restricción a B del orden $\leq_C$ de C y para cada par de elementos $x \in B$ e $y \in C \setminus B$ se cumple que $x \leq_C y$.

Vamos a comprobar que el par $(\Sigma, \leq)$ es un conjunto ordenado inductivo. Sea $\Lambda \in \Sigma$ un conjunto totalmente ordenado. Definimos el conjunto

$$X := \bigcup_{(B, \leq_B) \in \Lambda} B \subset A,$$

en el que vamos a construir un orden total $\leq_X$ que hace del par $(X, \leq_X)$ una cota superior de Λ. El orden $\leq_X$ se define así: para cada par de puntos $x, y \in X$ existen $(B, \leq_B)$ y $(C, \leq_C)$ tales que $x \in B$ e $y \in C$. Como Λ está totalmente ordenado, podemos suponer que $(B, \leq_B) \leq (C, \leq_C)$, por lo que $x, y \in C$ y decimos que $x \leq_X y$ si y sólo si $x \leq_C y$.

Veamos que la definición del orden $\leq_X$ no depende de los conjuntos B y C elegidos que contienen a x e y, respectivamente. En efecto, si $(D, \leq_D), (E, \leq_E) \in \Lambda$ son tales que $x \in D$ e $y \in E$ de nuevo podemos suponer que $(D, \leq_D) \leq (E, \leq_E)$, por lo que $x, y \in E$. Por ser Λ totalmente ordenado podemos suponer que $(E, \leq_E) \leq (C, \leq_C)$, luego el orden $\leq_E$ es la restricción de $\leq_C$, por lo que $x \leq_E y$ si y sólo si $x \leq_C y$.

Por la propia definición, $(X, \leq_X)$ es cota superior de Λ, lo que demuestra que Σ es un conjunto inductivo. Como estamos admitiendo la veracidad del Lema de Zorn, existe un elemento maximal $(M, \leq_M) \in (\Sigma, \leq)$ y basta probar que $M = A$. En caso contrario existe $\zeta \in A \setminus M$ y denotamos $N := M \cup \{\zeta\} \subset A$. Extendemos el orden $\leq_M$ a N mediante $x < \zeta, \forall x \in M$. Es evidente que $(N, \leq_N)$ está bien ordenado por estarlo $(M, \leq_M)$, luego $(M, \leq_M) < (N, \leq_N)$, contra la maximalidad de $(M, \leq_M)$. En conclusión, $M = A$ y hemos acabado.

(5) $\implies$ (1) Sea A un conjunto no vacío. Por la hipótesis existe un orden $\leq$ que hace del par $(A, \leq)$ un conjunto bien ordenado, y la aplicación

$$\varphi : \mathcal{P}(A) \setminus \varnothing \to A, X \mapsto \text{mín}(X)$$

cumple que $\varphi(X) \in X$ para cada $X \subset A$ no vacío. □

II.2. Principio de comparación de cardinales

Una pregunta muy natural acerca de los cardinales es la siguiente: dados dos conjuntos A y B, ¿es cierto que bien $\text{Card}(A) \leq \text{Card}(B)$ o bien $\text{Card}(B) \leq \text{Card}(A)$? Este es el llamado *Principio de comparación de cardinales* y vamos a demostrar que cualquiera de los enunciados del Teorema II.1.3 es equivalente al Principio de comparación de cardinales. Demostramos primero que el Lema de Zorn implica el Principio de comparación de cardinales. Demostrar la otra implicación requerirá introducir nueva terminología y desarrollar algunos resultados auxiliares.

Proposición II.2.1. *El Lema de Zorn implica el Principio de comparación de cardinales.*

Demostración. Sean A y B dos conjuntos y consideremos el conjunto

$$\mathcal{H} = \{(X, f_X) : X \subset A \text{ y } f_X : X \to B \text{ es una aplicación inyectiva}\}.$$

Definimos en $\mathcal{H}$ la relación de orden $(X, f_X) \leq (Y, g_Y)$ si $X \subset Y$ y $g_Y|_X = f_X$, y comprobamos que $(\mathcal{H}, \leq)$ es un conjunto inductivo. En efecto, sean $\Sigma \subset \mathcal{H}$ un subconjunto totalmente ordenado y la unión $C := \bigcup_{(X,f_X)\subset\Sigma} X$. Definimos la aplicación $f_C : C \to B, x \mapsto f_X(x)$ si $(X, f_X) \in \Sigma$ y $x \in X$. La definición de f_C tiene sentido pues si existe otro par $(Y, g_Y) \in \Sigma$ tal que $x \in Y$, podemos suponer, por estar Σ totalmente ordenado, que $(X, f_X) \leq (Y, g_Y)$, luego $g_Y|_X = f_X$ y, en particular, $f_X(x) = g_Y(x)$. Además f_C es inyectiva pues dados elementos $x, y \in C$ con $x \neq y$ existe $(X, f_X) \in \Sigma$ tal que $x, y \in X$ y, como f_X es inyectiva, $f_C(x) = f_X(x) \neq f_X(y) = f_C(y)$. Por tanto, $(C, f_C) \in \mathcal{H}$ y es una cota superior de Σ porque $f_C|_X = f_X$ para cada $(X, f_X) \in \Sigma$, por lo que $\mathcal{H}$ es inductivo. Aplicando el Lema de Zorn, existe por tanto un elemento maximal (M, f_M) de $\mathcal{H}$ y distinguimos varios casos.

Si $M = A$ entonces existe una aplicación inyectiva $f_A : A \to B$ o, lo que es lo mismo, $\mathrm{Card}(A) \leq \mathrm{Card}(B)$. Supongamos ahora que $M \neq A$ y distinguimos dos subcasos. Si $f_M(M) \neq B$ existen $\zeta \in A \setminus M$ e $y \in B \setminus f_M(M)$ lo que nos permite extender de modo inyectivo f_M al conjunto $N := M \cup \{\zeta\}$ mediante

$$f_N : N \to B, x \mapsto \begin{cases} f_M(x) & \text{si } x \neq \zeta, \\ y & \text{si } x = \zeta. \end{cases}$$

Por tanto $(N, f_N) \in \mathcal{H}$ y $(M, f_M) < (N, f_N)$, lo que contradice la maximalidad de (M, f_M). En consecuencia $f_M(M) = B$, por lo que $f_M : M \to B$ es biyectiva. Así, si $\mathtt{j} : M \to A$ es la inclusión, la composición $\mathtt{j} \circ (f_M)^{-1} : B \to A$ es una aplicación inyectiva, esto es, $\mathrm{Card}(B) \leq \mathrm{Card}(A)$. □

Observación II.2.2. El recíproco de II.2.1 es también cierto y lo probaremos en II.2.4. En consecuencia, el Principio de comparación de cardinales es equivalente a los enunciados del Teorema II.1.3. La demostración que proponemos se apoya en el siguiente resultado, debido a Hartogs, cuya prueba posponemos hasta el final de esta sección. Presentamos antes su enunciado y cómo emplearlo en la demostración de II.2.4.

Teorema II.2.3 (Teorema de Hartogs). *Para cada conjunto no vacío A existe un conjunto bien ordenado $(B, \leq_B)$ de modo que no existe ninguna aplicación inyectiva $B \hookrightarrow A$.*

Corolario II.2.4. *El Principio de comparación de cardinales implica el Principio de la buena ordenación de Zermelo.*

Demostración. Sea A un conjunto no vacío. Por el Teorema de Hartogs existe un conjunto bien ordenado $(B, \leq_B)$ de modo que no se cumple que $\mathrm{Card}(B) \leq \mathrm{Card}(A)$. Como admitimos el Principio de comparación de cardinales, $\mathrm{Card}(A) \leq \mathrm{Card}(B)$. Por tanto existe una aplicación inyectiva $f : A \to B$, y definimos una relación de orden en A mediante: dados $x, y \in A$, se tiene $x \leq_A y$ si y sólo si $f(x) \leq_B f(y)$. El par $(A, \leq_A)$ es un conjunto bien ordenado, pues dado cualquier subconjunto no vacío $C \subset A$, su imagen $f(C)$ es un subconjunto no vacío de B, que está bien ordenado, luego existe $b := \mín(f(C)) \in f(C)$. Como $f|_C : C \to f(C)$ es biyectiva, existe un único elemento $c \in C$ tal que $f(c) = b$ y se cumple que $c = \mín(C)$. En efecto, dado $x \in C$, su imagen $f(x) \in f(C)$, luego $f(c) = b \leq_B f(x)$, o sea, $c \leq_A x$. □

La demostración del Teorema de Hartogs exige introducir previamente algunas nociones y resultados auxiliares.

Definición y Observación II.2.5. (1) Sean $(A, \leq)$ un conjunto parcialmente ordenado y $a \in A$. El subconjunto $A_a := \{x \in A : x < a\}$ se llama *sección inicial de A determinada por a*. Obsérvese que si $a, b \in A$ cumplen que $a < b$, entonces $A_a = \{x \in A_b : x < a\}$, es decir, A_a es también una sección inicial de $(A_b, \leq)$.

(2) Dados un conjunto totalmente ordenado $(A, \leq)$ y un subconjunto $B \subset A$, se dice que B es un *segmento inicial* de A si para cada $(x, y) \in B \times (A \setminus B)$ se cumple que $x < y$.

(3) Toda sección inicial de un conjunto totalmente ordenado $(A, \leq)$ es un segmento inicial de $(A, \leq)$. En efecto, dados $a \in A$ y $(x, y) \in A_a \times (A \setminus A_a)$ se cumple que $x < a$ pero y no es menor que a. Como el orden es total, $a \leq y$, luego $x < a \leq y$ y por ello $x < y$.

(4) Dados conjuntos parcialmente ordenados $(A, \leq_A)$ y $(B, \leq_B)$ se dice que una aplicación $f : A \to B$ es *creciente* si para cada $x, y \in A$ tales que $x < y$ se cumple que $f(x) < f(y)$.

(5) Se dice que una aplicación $f : A \to B$ entre los conjuntos parcialmente ordenados $(A, \leq_A)$ y $(B, \leq_B)$ es un *isomorfismo de conjuntos parcialmente ordenados* si es biyectiva, creciente y su inversa también es creciente. Si entre dos conjuntos parcialmente ordenados $(A, \leq_A)$ y $(B, \leq_B)$ existe un isomorfismo se dice que son *isomorfos*, lo que se denota $(A, \leq_A) \simeq (B, \leq_B)$. Un *automorfismo* del conjunto parcialmente ordenado $(A, \leq_A)$ es un isomorfismo entre $(A, \leq_A)$ y él mismo. Es claro que si $(A, \leq_A) \simeq (B, \leq_B) \simeq (C, \leq_C)$, entonces $(A, \leq_A) \simeq (C, \leq_C)$.

(6) Supongamos que $(A, \leq_A)$ y $(B, \leq_B)$ son totalmente ordenados. Entonces, la condición de que $f^{-1} : B \to A$ sea creciente en la definición anterior es consecuencia de las demás. En efecto, en caso contrario existirían $b_1, b_2 \in B$ tales que $b_1 <_B b_2$ pero no se cumple que $a_1 := f^{-1}(b_1)$ es menor que $a_2 := f^{-1}(b_2)$. Entonces, como

el orden $\leq_A$ es total y f es inyectiva, necesariamente $a_2 < a_1$ luego, como f es creciente, $b_2 = f(a_2) <_B f(a_1) = b_1$ y esto es una contradicción.

(7) Si tenemos dos conjuntos totalmente ordenados isomorfos $(A, \leq_A) \simeq (B, \leq_B)$ a través del isomorfismo $f : A \to B$ y $x \in A$, entonces $(A_x, \leq_A)$ es isomorfo a $(B_{f(x)}, \leq_B)$ tomando $f|_{A_x}$ como isomorfismo. En efecto es creciente y está bien definida pues si tomamos $a_1, a_2 \in A_x$ con $a_1 < a_2 < x$, tenemos que $f|_{A_x}(a_1) = f(a_1) < f(a_2) = f|_{A_x}(a_2)$ y ambos son menores que $f(x)$. Además, es inyectiva pues si $a_1 \neq a_2$ son elementos de A_x, entonces $f|_{A_x}(a_1) = f(a_1) \neq f(a_2) = f|_{A_x}(a_2)$. Para comprobar que es sobreyectiva, consideramos un elemento $b \in B_{f(x)}$. Como f es isomorfismo, existe $a \in A$ tal que $f(a) = b < f(x)$ y tenemos que f^{-1} es creciente, luego $a < x$ y $a \in A_x$. Por el apartado anterior, tenemos que $f|_{A_x}^{-1}$ es creciente al ser $(A_x, \leq_A)$ y $(B, \leq_B)$ totalmente ordenados.

Lema II.2.6. *(1) Todo conjunto bien ordenado $(A, \leq)$ está totalmente ordenado.*

(2) Sean $(A, \leq)$ un conjunto bien ordenado y $B \subsetneq A$ un segmento inicial de A distinto de A. Entonces B es una sección inicial de A.

(3) Sean $(A, \leq)$ un conjunto bien ordenado y $f : A \to A$ una aplicación creciente. Entonces $a \leq f(a)$ para cada $a \in A$.

(4) Si $(A, \leq)$ es un conjunto bien ordenado, entonces no es isomorfo a ninguna de sus secciones iniciales.

(5) Si $(A, \leq)$ es un conjunto bien ordenado entonces la aplicación identidad $id_A : A \to A$ es el único automorfismo de $(A, \leq)$.

(6) Si $(A, \leq_A)$ y $(B, \leq_B)$ son conjuntos bien ordenados isomorfos, entonces existe un único isomorfismo entre ellos.

Demostración. (1) Dados $x, y \in A$, el subconjunto $B := \{x, y\}$ de A tiene mínimo por estar A bien ordenado. Si, por ejemplo, $x := \min(B)$, entonces $x \leq y$.

(2) El conjunto $A \setminus B$ es no vacío, por hipótesis, luego existe $a := \min(A \setminus B)$, pues $(A, \leq)$ está bien ordenado. Vamos a demostrar que B coincide con la sección inicial A_a. Si $x \in A_a$ entonces $x < a = \min(A \setminus B)$, luego $x \notin A \setminus B$ y, por tanto, $b \in B$. Para comprobar la inclusión recíproca supongamos, por reducción al absurdo, que existe $x \in B \setminus A_a$. Entonces, al estar A totalmente ordenado por el apartado (1), $a \leq x \in B$ y, como B es segmento inicial, $a \in B$, lo que es falso.

(3) Supongamos que existe algún elemento $a \in A$ que no cumple $a \leq f(a)$. Como A está totalmente ordenado, $f(a) < a$ y, en consecuencia, el conjunto $C := \{x \in A : f(x) < x\}$ es no vacío y existe $c := \min(C)$. Como f es creciente y $f(c) < c$ se cumple que $f(f(c)) < f(c)$, luego $f(c) \in C$ y eso contradice que c sea el menor elemento de C pues $f(c) < c$.

(4) Supongamos, por reducción al absurdo, que existen $a \in A$ y un isomorfismo de conjuntos bien ordenados $f : A \to A_a$. En particular $f : A_a \to A_a$ es una aplicación creciente, luego por el apartado anterior, $a \leq f(a)$. Esto es absurdo pues $f(a) \in A_a$.

(5) Sean $f : A \to A$ un automorfismo de $(A, \leq)$ y $a \in A$. Por el apartado (3), $a \leq f(a)$. Aplicando (3) al isomorfismo $f^{-1} : A \to A$ deducimos que $x \leq f^{-1}(x)$ para cada $x \in A$ luego, en particular, $f(a) \leq f^{-1}(f(a)) = a \leq f(a)$, es decir, $f(a) = a$. Por tanto, $f = id_A$.

(6) Sean $f : A \to B$ y $g : A \to B$ dos isomorfismos de conjuntos bien ordenados. Entonces la composición $g^{-1} \circ f : A \to A$ es un automorfismo del conjunto bien ordenado $(A, \leq_A)$ luego, por el apartado anterior, $g^{-1} \circ f = id_A$, esto es, $f = g$. □

Teorema II.2.7. *Sean $(A, \leq_A)$ y $(B, \leq_B)$ dos conjuntos bien ordenados. Entonces se cumple una y sólo una de las siguientes opciones:*

(I) Los conjuntos $(A, \leq_A)$ y $(B, \leq_B)$ son isomorfos.

(II) Existe $b \in B$ tal que $(A, \leq_A)$ es isomorfo a la sección $(B_b, \leq_B)$ de $(B, \leq_B)$.

(III) Existe $a \in A$ tal que $(B, \leq_B)$ es isomorfo a la sección $(A_a, \leq_A)$ de $(A, \leq_A)$.

Demostración. Consideremos el conjunto

$$F := \{(a, b) \in A \times B : (A_a, \leq_A) \simeq (B_b, \leq_B)\}$$

y vamos a demostrar que se trata de una aplicación cuyo dominio es un segmento inicial de $(A, \leq_A)$, cuya imagen es un segmento inicial de $(B, \leq_B)$ y que es un isomorfismo entre estos segmentos iniciales. Después probaremos que estos segmentos iniciales, que si no coinciden con el conjunto total son, por el Lema II.2.6, secciones iniciales, no pueden ser simultáneamente distintos de A el primero y de B el segundo.

Comenzamos probando que F es una aplicación. Sean $(a, b_1), (a, b_2) \in F$. Debemos probar que $b_1 = b_2$. Como la isomorfía de conjuntos ordenados es transitiva, las secciones iniciales $(B_{b_1}, \leq_B)$ y $(B_{b_2}, \leq_B)$ son isomorfas. Si $b_1 \neq b_2$, por ejemplo $b_1 < b_2$, entonces $(B_{b_1}, \leq_B)$ es una sección inicial de $(B_{b_2}, \leq_B)$ y $(B_{b_1}, \leq_B) \simeq (B_{b_2}, \leq_B)$, lo que contradice II.2.6 (4). Por tanto, $b_1 = b_2$.

Veamos ahora que el dominio $\mathrm{dom}(F)$ de F es un segmento inicial de $(A, \leq_A)$. Hemos de probar que si $(x, y) \in \mathrm{dom}(F) \times (A \setminus \mathrm{dom}(F))$, entonces $x < y$. Desde luego $x \neq y$, pues $x \in \mathrm{dom}(F)$ e $y \in A \setminus \mathrm{dom}(F)$. Supongamos que $y < x \in \mathrm{dom}(F)$. Sean $b \in B$ (que existe por estar x en el dominio de A) tal que exista un isomorfismo $f : A_x \to B_b$ entre las secciones $(A_x, \leq_A)$ y $(B_b, \leq_B)$. Como $y \in A_x$ tiene sentido $f(y) \in B_b$ y la restricción $f|_{A_y} : A_y \to B_{f(y)}$ es un isomorfismo gracias al último apartado de II.2.5, por lo que $(y, f(y)) \in F$, es decir, $y \in \mathrm{dom}(F)$, lo que es falso. Como el orden en A es total, se concluye que $x < y$.

Comprobemos ahora que la imagen $\mathrm{im}(F)$ de F es un segmento inicial de $(B, \leq_b)$. Probaremos que si $(z, t) \in \mathrm{im}(F) \times (B \setminus \mathrm{im}(F))$, entonces $z < t$. Supongamos lo contrario.

Como el orden en B es total y como $z \neq t$, tenemos que $t < z \in \mathrm{im}(F)$ y existen por tanto $a \in A$ y un isomorfismo $f : A_a \to B_z$ entre las secciones $(A_a, \leq_A)$ y $(B_z, \leq_B)$. Como $t \in B_z$ existe $x \in A_a$ tal que $f(x) = t$ y $f|_{A_x} : A_x \to B_{f(x)}$ es un isomorfismo, por lo que $(x, t) = (x, f(x)) \in F$, o sea, $t \in \mathrm{im}(F)$, lo que es falso.

Veamos a continuación que $F : \mathrm{dom}(F) \to \mathrm{im}(F)$ es un isomorfismo de conjuntos bien ordenados cuando en $\mathrm{dom}(F)$ e $\mathrm{im}(F)$ se consideran los órdenes inducidos $\leq_A$ y $\leq_B$, respectivamente. En efecto, veamos primero que F es inyectiva. Hemos de probar que si $(a_1, b), (a_2, b) \in F$, entonces $a_1 = a_2$. Obsérvese que las secciones iniciales $(A_{a_1}, \leq_A)$ y $(A_{a_2}, \leq_A)$ son isomorfas, pues ambas lo son a la sección inicial $(B_b, \leq_B)$. Si $a_1 \neq a_2$ tenemos, por ser A totalmente ordenado, por ejemplo, $a_1 < a_2$, con lo que $(A_{a_1}, \leq_A)$ es una sección inicial del conjunto bien ordenado $(A_{a_2}, \leq_A)$ y $(A_{a_1}, \leq_A) \simeq (A_{a_2}, \leq_A)$, lo que contradice el apartado (4) del Lema II.2.6. Por tanto, $a_1 = a_2$.

Como evidentemente $F : \mathrm{dom}(F) \to \mathrm{im}(F)$ es sobreyectiva, para probar que es un isomorfismo basta comprobar, en virtud del apartado (6) de II.2.5, que F es creciente. Sean $a_1, a_2 \in \mathrm{dom}(F)$ tales que $a_1 < a_2$. Esto implica, por II.2.5 (1), que A_{a_1} es una sección inicial de A_{a_2}. Puesto que a_1 y a_2 son elementos del dominio de F existen, por el apartado (6) del Lema II.2.6, isomorfismos únicos

$$h : A_{a_1} \to B_{F(a_1)} \text{ y } g : A_{a_2} \to B_{F(a_2)}.$$

Como A_{a_1} es una sección inicial de A_{a_2}, su imagen $g(A_{a_1})$ es una sección inicial de $B_{F(a_2)}$; de hecho, $g(A_{a_1}) = B_{g(a_1)}$, por lo que $g|_{A_{a_1}} : A_{a_1} \to B_{g(a_1)}$ es un isomorfismo de conjuntos bien ordenados. Por tanto, $B_{F(a_1)}$ y $B_{g(a_1)}$ son secciones iniciales de $(B, \leq_B)$ isomorfas entre sí, porque ambas lo son a A_{a_1}. Se deduce entonces del apartado (4) del Lema II.2.6 que ambas secciones iniciales coinciden, luego $F(a_1) = g(a_1)$. Como $a_1 \in A_{a_2}$ resulta que $g(a_1) \in B_{F(a_2)}$, esto es, $g(a_1) < F(a_2)$. Así, finalmente, $F(a_1) = g(a_1) < F(a_2)$, lo que completa la demostración de que F es un isomorfismo entre los segmentos iniciales $\mathrm{dom}(F)$ e $\mathrm{im}(F)$.

Supongamos que $\mathrm{dom}(F) \neq A$ e $\mathrm{im}(F) \neq B$. Entonces, se deduce del apartado (2) del Lema II.2.6 que tanto $\mathrm{dom}(F) \neq A$ como $\mathrm{im}(F) \neq B$ son secciones iniciales de $(A, \leq_A)$ y $(B, \leq_B)$, es decir, existen $a \in A$ y $b \in B$ tales que $\mathrm{dom}(F) = A_a$ e $\mathrm{im}(F) = B_b$. Esto significa que $F : A_a \to B_b$ es un isomorfismo, luego $(a, b) \in F$ y, en particular, $a \in \mathrm{dom}(F) = A_a$, lo que es falso.

Por tanto, bien $A = \mathrm{dom}(F)$ en cuyo caso se cumple (i) o (ii), bien $A \neq \mathrm{dom}(F)$ y $B = \mathrm{im}(F)$, en cuyo caso se cumple (iii), lo que concluye la demostración, ya que las tres opciones son mutuamente excluyentes pues, según vimos en el Lema II.2.6 (4), ningún conjunto bien ordenado es isomorfo a alguna de sus secciones iniciales □

Demostración del Teorema II.2.3. Consideremos el conjunto

$$\mathcal{H} := \{(M, \leq_M) : M \subset A \text{ y } (M, \leq_M) \text{ es un conjunto bien ordenado}\},$$

que no es vacío pues basta tomar $a \in A$ y considerar en $M := \{a\}$ es único orden posible. Definimos en $\mathcal{H}$ la relación de equivalencia "ser isomorfos como conjuntos ordenados", que

denotamos $\sim$. Denotamos la clase de equivalencia de $(M, \leq_M) \in \mathcal{H}$ mediante $[(M, \leq_M)]_\sim$. En el conjunto cociente $\mathcal{W} := \mathcal{H}/\sim$ consideramos la siguiente relación de orden parcial estricto:

$[(M, \leq_M)]_\sim \prec [(N, \leq_N)]_\sim$ si $(M, \leq_M)$ es isomorfo a una sección inicial de $(N, \leq_N)$.

Es evidente que la definición no depende de los representantes elegidos y hemos de comprobar que se trata, de hecho, de una relación de orden. La transitividad se sigue de que una sección inicial de otra sección inicial de un conjunto parcialmente ordenado $(M, \leq_M)$ es una sección inicial de $(M, \leq_M)$. Además, si $[(M, \leq_M)]_\sim \prec [(N, \leq_N)]_\sim \prec [(M, \leq_M)]_\sim$, la transitividad lleva a $[(M, \leq_M)]_\sim \prec [(M, \leq_M)]_\sim$, esto es, a que $(M, \leq_M)$ es isomorfo a una de sus secciones iniciales, lo que no es posible entre conjuntos bien ordenados. Hemos probado la antirreflexividad, lo que concluye que se trata, en efecto, de una relación de orden estricto.

Comprobemos que $(\mathcal{W}, \sim)$ es un conjunto bien ordenado. Observemos primero que está totalmente ordenado, pues eso es lo que dice el Teorema II.2.7. Ahora, sea $\mathcal{V}$ un subconjunto no vacío de $\mathcal{W}$ y debemos comprobar que posee mínimo. Tomamos un elemento arbitrario $[(M, \leq_M)]_\sim \in \mathcal{V}$ y consideramos

$$N := \{x \in M : [(M_x, \leq_M)]_\sim \in \mathcal{V}\}.$$

Si $N = \varnothing$ entonces $[(M, \leq_M)]_\sim = \min(\mathcal{V})$. En efecto, en caso contrario y puesto que $(\mathcal{W}, \prec)$ es un conjunto totalmente ordenado, existiría $[(P, \leq_P)]_\sim \in \mathcal{V}$ tal que $[(P, \leq_P)]_\sim \prec [(M, \leq_M)]_\sim$. Esto significa que $(P, \leq_P)$ es isomorfo a una sección inicial de M, esto es, existe $x \in M$ tal que $[(M_x, \leq_M)]_\sim \simeq [(P, \leq_P)]_\sim \in \mathcal{V}$, luego $x \in N$, contradicción.

Si N no es vacío posee mínimo, que denotamos $x := \min(N)$ y comprobamos que $[(M_x, \leq_M)]_\sim = \min(\mathcal{V})$. En caso contrario existiría $y \in M$ tal que $[(M_y, \leq_M)]_\sim \in \mathcal{V}$, luego $y \in N$, y $[(M_y, \leq_M)]_\sim \prec [(M_x, \leq_M)]_\sim$. Esto último significa que $(M_y, \leq_M)$ es una sección inicial de $(M_x, \leq_M)$, por lo que $y < x$, lo que contradice la minimalidad de x en N.

Para terminar nos basta demostrar que no existe ninguna aplicación inyectiva $\mathcal{W} \hookrightarrow A$. Supongamos, por reducción al absurdo, que existe una aplicación inyectiva $f : \mathcal{W} \hookrightarrow A$. El conjunto imagen $M := f(\mathcal{W}) \subset A$ admite un buen orden inducido por el de $\mathcal{W}$: dados $x, y \in M$ se define $x <_M y$ si $f^{-1}(x) \prec f^{-1}(y)$. En consecuencia, $(\mathcal{W}, \prec)$ es isomorfo a $(M, \leq_M) \in \mathcal{H}$ que resulta bien ordenado.

Consideramos ahora la sección inicial de $\mathcal{W}$ determinada por la clase de equivalencia $[(M, \leq_M)]_\sim \in \mathcal{W}$ y observamos que, por definición,

$$\begin{aligned}\mathcal{W}_{[(M,\leq_M)]_\sim} &= \{[(X, \leq_X)]_\sim \in \mathcal{W} : [(X, \leq_X)]_\sim \prec [(M, \leq_M)]_\sim\} \\ &= \{[(M_x, \leq_M)]_\sim : x \in M\}.\end{aligned}$$

Comprobaremos a continuación que este último conjunto, con el orden $\prec$, es isomorfo a $(M, \leq_M)$. Hecho esto resultará que el conjunto bien ordenado $(\mathcal{W}, \prec)$ es isomorfo a una de sus secciones iniciales:

$$(\mathcal{W}, \prec) \simeq (M, \leq_M) \simeq \{[(M_x, \leq_M)]_\sim : x \in M\} = (\mathcal{W}_{[(M,\leq_M)]_\sim}, \prec).$$

El isomorfismo buscado entre los conjuntos ordenados $(M, \leq_M)$ y $(\{[(M_x, \leq_M)]_\sim : x \in M\}, \prec)$ viene dado por

$$\varphi : M \to \{[(M_x, \leq_M)]_\sim : x \in M\}, x \mapsto [(M_x, \leq_M)]_\sim,$$

que es evidentemente una aplicación sobreyectiva. También es inyectiva y creciente pues si x e y son elementos de M con $x \neq y$ entonces, puesto que M es totalmente ordenado por ser bien ordenado, podemos suponer $x < y$, luego $x \in M_y \setminus M_x$ y así M_x es sección inicial de M_y, esto es, $[(M_x, \leq_M)]_\sim \prec [(M_y, \leq_M)]_\sim$ y $[(M_x, \leq_M)]_\sim \neq [(M_y, \leq_M)]_\sim$. $\square$

Capítulo III

Aplicaciones

III.1. Existencia y unicidad del cierre algebraico de un cuerpo

Definición y Proposición III.1.1. Se dice que un cuerpo E es *algebraicamente cerrado* si cumple alguna de las siguientes condiciones equivalentes y, por tanto, todas:

(1) *Todo polinomio $f \in E[\mathtt{t}]$ de grado ≥ 1 tiene alguna raíz en E.*

(2) *Todo polinomio $f \in E[\mathtt{t}]$ de grado ≥ 1 factoriza en $E[\mathtt{t}]$ como producto de factores lineales.*

(3) *Existe un subcuerpo $K \subset E$ tal que la extensión $E|K$ es algebraica y cada $f \in K[\mathtt{t}]$ de grado ≥ 1 factoriza en $E[\mathtt{t}]$ como producto de factores lineales.*

(4) *El cuerpo E no admite extensiones algebraicas no triviales.*

Demostración. (1) $\Longrightarrow$ (2) Argumentamos por inducción sobre $n := \deg(f)$. Si $n = 1$ nada hay que probar. Si $n > 1$, sea $\alpha_1 \in E$ raíz de f. Entonces existe $g \in E[\mathtt{t}]$ de grado $n-1$ tal que $f(\mathtt{t}) = (\mathtt{t}-\alpha_1)g(\mathtt{t})$ y, por la hipótesis de inducción, $g(\mathtt{t}) = a\prod_{i=2}^{n}(\mathtt{t}-\alpha_i)$ para ciertos $a, \alpha_2, \ldots, \alpha_n \in E$. Entonces,

$$f(\mathtt{t}) = (\mathtt{t}-\alpha_1)g(\mathtt{t}) = a\prod_{i=1}^{n}(\mathtt{t}-\alpha_i).$$

Para la implicación (2) $\Longrightarrow$ (3) basta elegir $K := E$.

(3) $\Longrightarrow$ (4) Sean $L|E$ una extensión algebraica y $u \in L$. Como $L|E$ y $E|K$ son extensiones algebraicas, $L|K$ también lo es, así que u es algebraico sobre K. Por hipótesis, el polinomio mínimo $P_{K,u} \in K[\mathtt{t}]$ de u sobre K factoriza en $E[\mathtt{t}]$ como producto de factores lineales, luego $\mathtt{t} - u \in E[\mathtt{t}]$, o sea, $u \in E$, por lo que $E = L$.

(4) $\Longrightarrow$ (1) Sea $f \in E[\mathtt{t}]$ con $\deg(f) \geq 1$. Elegimos un factor irreducible g de f en $E[\mathtt{t}]$. El cociente $L := E[\mathtt{t}]/(g \cdot E[\mathtt{t}])$ es un cuerpo, por ser g irreducible y $E[\mathtt{t}]$

un dominio de ideales principales y, de hecho, $L|E$ es una extensión de cuerpos porque la aplicación $\mathtt{j} : E \to L, a \mapsto a + gE[\mathtt{t}]$ es homomorfismo de cuerpos (inyectivo). Es inmediato comprobar que, si $d := \deg(g)$, una base de L como E-espacio vectorial es

$$\mathcal{B} := \{1 + gE[\mathtt{t}], \mathtt{t} + gE[\mathtt{t}], \ldots, \mathtt{t}^{d-1} + gE[\mathtt{t}]\},$$

luego $L|E$ es una extensión finita y $u := \mathtt{t} + gE[\mathtt{t}] \in L$ cumple que $g(u) = 0$, luego $f(u) = 0$ y, como E no admite extensiones algebraicas no triviales, tenemos $L = E$ y $u \in E$. □

Definición III.1.2. Dado un cuerpo K, se dice que una extensión L es un *cierre* o *clausura algebraica* de K si $L|K$ es algebraica y L es algebraicamente cerrado.

Ya se puede formular con precisión el problema central en lo que queda de sección. Dado un cuerpo K, queremos construir un cierre algebraico suyo. Antes de demostrar su existencia necesitamos algunas nociones adicionales sobre cardinalidad.

Definición III.1.3. Un conjunto se dice *numerable* si es equipotente con algún subconjunto de $\mathbb{N}$.

Proposición III.1.4. *Sea $\mathbb{N}$ el conjunto de los números naturales. Entonces:*

(1) Si X es un conjunto infinito, existe una aplicación inyectiva $\mathbb{N} \hookrightarrow X$.

(2) Dados dos conjuntos numerables infinitos, su unión es un conjunto numerable infinito.

Demostración. (1) Como X es infinito, existen $x_0 \in X$ y una aplicación biyectiva $f : X \to X \setminus \{x_0\}$. Consideremos el conjunto $Y := \{f^k(x_0) : k \in \mathbb{N}\}$, donde f^k es la composición de f consigo misma k veces. La inyectividad de f implica la de f^k para cada $k \in \mathbb{N}$. Además, $\mathrm{im}(f^k) \subset \mathrm{im}(f) = X \setminus \{x_0\}$.

En particular, $f^m(x_0) \neq f^n(x_0)$ si $m \neq n$. En efecto, si $f^m(x_0) = f^n(x_0)$, y podemos suponer $m < n$, se tiene

$$f^m(x_0) = f^n(x_0) = f^m(f^{n-m}(x_0)),$$

y de la inyectividad de f^m se deduce que $f^{n-m}(x_0) = x_0$, que es falso porque $\mathrm{im}(f^{n-m}) \subset X \setminus x_0$, esto es, $x_0 \notin \mathrm{im}(f^{n-m})$.

Así, la aplicación $\mathbb{N} \hookrightarrow Y, k \mapsto f^k(x_0)$ es inyectiva y su composición con la inclusión $\mathtt{j} : Y \hookrightarrow X$ proporciona una aplicación inyectiva $\mathbb{N} \to X$.

(2) Sean A y B conjuntos numerables infinitos. Sea $C := B \setminus A$, que cumple $A \cup B = A \sqcup C$. La inclusión $\mathtt{j} : A \hookrightarrow A \sqcup C$ es inyectiva, luego, por el Teorema de Cantor-Bernstein, es suficiente encontrar una aplicación inyectiva $A \sqcup C \hookrightarrow A$. Por la Proposición I.2.1(6) existe una biyección entre A y $\mathbb{N} \times \mathbb{N}$, luego basta encontrar una aplicación inyectiva $A \sqcup C \hookrightarrow \mathbb{N} \times \mathbb{N}$. Ahora bien, existen aplicaciones inyectivas $f : A \hookrightarrow \mathbb{N}$ y $g : C \hookrightarrow \mathbb{N}$, por lo que la aplicación

$$h : A \sqcup C \hookrightarrow \mathbb{N} \times \mathbb{N}, x \mapsto \begin{cases} (f(x), 1) & \text{si } x \in A, \\ (g(x), 2) & \text{si } x \in C \end{cases}$$

es inyectiva. □

Proposición III.1.5. *(1) Sean X un conjunto infinito y F un conjunto finito. Entonces* $\mathrm{Card}(X) = \mathrm{Card}(X \cup F)$.

(2) Sea X un conjunto infinito. Entonces $\mathrm{Card}(X) = \mathrm{Card}(X \times \{0,1\})$.

(3) Sean X, Y dos conjuntos tales que $\mathrm{Card}(Y) \leq \mathrm{Card}(X)$. *Entonces* $\mathrm{Card}(X \cup Y) \leq \mathrm{Card}(X \times \{0,1\})$ *y se cumple* $\mathrm{Card}(X \cup Y) = \mathrm{Card}(X \times \{0,1\})$ *si* $\mathrm{Card}(X) = \mathrm{Card}(Y)$ *y* $X \cap Y = \varnothing$.

Demostración. (1) Podemos suponer que $F \cap X = \varnothing$, pues basta sustituir F por $F \setminus X$. Si $F = \varnothing$ no hay nada que demostrar. Si $F \neq \varnothing$, por ser un conjunto finito, tenemos que $F \simeq F_n \subset \mathbb{N}$ donde $F_n := \{1, \ldots, n\}$. Por el Teorema de Cantor-Bernstein basta demostrar que existe una aplicación inyectiva $\mathtt{j}_n : X \sqcup F_n \hookrightarrow X$. Como X es infinito, existen $x_0 \in X$ y una biyección $f : X \to X \setminus \{x_0\}$. Por ello también es biyectiva la aplicación $\mathtt{j}_1 : X \sqcup F_1 \hookrightarrow X$ definida por

$$\mathtt{j}_1(x) := \begin{cases} f(x) & \text{si } x \in X, \\ x_0 & \text{si } x = 1. \end{cases}$$

Supongamos que existe una aplicación inyectiva $\mathtt{j}_n : X \sqcup F_n \hookrightarrow X$. La composición $f \circ \mathtt{j}_n : X \sqcup F_n \hookrightarrow X \setminus \{x_0\}$ es también inyectiva, luego lo es

$$\mathtt{j}_{n+1} : X \sqcup F_{n+1} \hookrightarrow X, x \mapsto \begin{cases} f(\mathtt{j}_n(x)) & \text{si } x \neq n+1, \\ x_0 & \text{si } x = n+1. \end{cases}$$

(2) Por el Teorema de Cantor-Bernstein es suficiente demostrar que existe una aplicación inyectiva $X \times \{0,1\} \hookrightarrow X$. Comenzamos probando que no es vacío el conjunto Σ formado por todos los pares (Y, f) donde $Y \subset X$ es un subconjunto infinito y $f : Y \times \{0,1\} \hookrightarrow Y$ es una aplicación inyectiva. Por el apartado (1) de la Proposición III.1.4 existe una aplicación inyectiva $\mathtt{j} : \mathbb{N} \hookrightarrow X$ y, por tanto, $Y_0 := \mathtt{j}(\mathbb{N}) \simeq \mathbb{N}$ es infinito numerable. Por esto último sabemos que $Y_0 \times \{0,1\} \simeq \mathbb{N} \times \{0,1\}$. Además, es trivial la inyección $\mathbb{N} \times \{0,1\} \hookrightarrow \mathbb{N} \times \mathbb{N}$. Por el apartado (6) de la Proposición I.2.1, sabemos que $\mathbb{N} \times \mathbb{N} \simeq \mathbb{N}$ por lo que existe una aplicación inyectiva $f_0 : Y_0 \times \{0,1\} \hookrightarrow Y_0$ y el par $(Y_0, f_0) \in \Sigma$, así que esta familia no es vacía. Definimos en ella la relación de orden $(Y_1, f_1) \preceq (Y_2, f_2)$ si $Y_1 \subset Y_2$ y $f_2|_{Y_1} = f_1$.

Vamos a demostrar, utilizando el Lema de Zorn, que Σ tiene un elemento maximal. Para ello basta observar que, dado un subconjunto totalmente ordenado $\mathcal{C} := \{(Y_i, f_i) : i \in I\}$ de Σ, el par (Y, f), donde

$$Y := \bigcup_{i \in I} Y_i \text{ y } f : Y \times \{0,1\} \hookrightarrow Y, (y, j) \mapsto f_i(y, j) \text{ si } y \in Y_i,$$

es cota superior de $\mathcal{C}$.

Sea $(Y, f) \in \Sigma$ un elemento maximal. Es suficiente probar que $\mathrm{Card}(Y) = \mathrm{Card}(X)$. Hecho esto, tomamos una biyección $g : X \to Y$ y la aplicación

$$X \times \{0,1\} \hookrightarrow X, (x,j) \mapsto g^{-1}(f(g(x),j))$$

es inyectiva, como queríamos.

Supongamos pues, por reducción al absurdo, que $\mathrm{Card}(Y) \neq \mathrm{Card}(X)$, es decir, $\mathrm{Card}(Y) < \mathrm{Card}(X)$. Se deduce del primer apartado que $X \setminus Y$ también es infinito, pues en caso contrario, $\mathrm{Card}(Y) = \mathrm{Card}(Y \cup (X \setminus Y)) = \mathrm{Card}(X)$, lo que sería absurdo. Por el apartado (1) de la Proposición III.1.4, $\mathbb{N}$ es isomorfo a un subconjunto $Z \subset X \setminus Y$. Repitiendo el argumento anterior para Y, por el apartado (6) de la Proposición I.2.1 existe una aplicación inyectiva $h : Z \times \{0,1\} \hookrightarrow Z$. De este modo, la aplicación

$$F : (Y \sqcup Z) \times \{0,1\} \hookrightarrow Y \sqcup Z, u \mapsto \begin{cases} f(u) & \text{si } u \in Y \times \{0,1\} \\ h(u) & \text{si } u \in Z \times \{0,1\} \end{cases}$$

es inyectiva e $(Y \sqcup Z, F) \in \Sigma$ cumple $(Y, f) \prec (Y \sqcup Z, F)$, lo que es absurdo.

(3) Por hipótesis, existe una inyección $f : Y \hookrightarrow X$. Entonces es evidente que la aplicación

$$F : X \cup Y \hookrightarrow X \times \{0,1\}, x \mapsto \begin{cases} (x,0) & \text{si } x \in X \\ (f(x),1) & \text{si } x \in Y \setminus X \end{cases}$$

es inyectiva.

Para la segunda parte es suficiente ver que, si la aplicación f es biyectiva y X e Y son disjuntos, entonces F es una biyección.

□

Corolario III.1.6. *Sean X un conjunto, $Y \subset X$ un subconjunto y $Z := X \setminus Y$. Supongamos que Y es infinito y $\mathrm{Card}(Z) < \mathrm{Card}(X)$. Entonces $\mathrm{Card}(Y) = \mathrm{Card}(X)$.*

Demostración. Supongamos primero que Z es finito. Entonces, por la Proposición III.1.5,

$$\mathrm{Card}(Y) = \mathrm{Card}(Y \cup Z) = \mathrm{Card}(X).$$

Supongamos ahora que Z es infinito y, por el Principio de comparación de cardinales, o bien $\mathrm{Card}(Z) \leq \mathrm{Card}(Y)$ o bien $\mathrm{Card}(Y) < \mathrm{Card}(Z)$. En el primer caso, empleando los apartados (2) y (3) de la Proposición III.1.5, se tiene

$$\mathrm{Card}(X) = \mathrm{Card}(Y \sqcup Z) \leq \mathrm{Card}(Y \times \{0,1\}) = \mathrm{Card}(Y)$$

y hemos acabado, mientras que en el segundo

$$\mathrm{Card}(X) = \mathrm{Card}(Y \sqcup Z) \leq \mathrm{Card}(Z \times \{0,1\}) = \mathrm{Card}(Z) < \mathrm{Card}(X),$$

lo que es absurdo. □

Corolario III.1.7. *(1) Si X es un conjunto infinito,* $\mathrm{Card}(X) = \mathrm{Card}(X \times X)$.

(2) Si X es un conjunto infinito y n es un entero positivo, $\mathrm{Card}(X) = \mathrm{Card}(X^n)$.

Demostración. (1) Por la Proposición III.1.4 (1), X contiene un conjunto numerable Y y, por la Proposición I.2.1, sabemos que existe una biyección $f_0 : Y \to Y \times Y$. Consideremos el conjunto Σ formado por todos los pares (A, f), donde $A \subset X$ es un subconjunto infinito y $f : A \to A \times A$ es una biyección. Vemos que Σ es no vacío ya que $(Y, f_0) \in \Sigma$.

Definimos en Σ la relación de orden $(A_1, f_1) \preceq (A_2, f_2)$ si $A_1 \subset A_2$ y $f_2|_{A_1} = f_1$ y vamos a probar, utilizando el Lema de Zorn, que Σ tiene un elemento maximal. Para ello, basta comprobar que, dado un subconjunto totalmente ordenado $\mathcal{C} := \{(A_i, f_i) : i \in I\} \subset \Sigma$, el par (A, f), donde

$$A := \bigcup_{i \in I} A_i \text{ y } f : A \to A \times A, a \mapsto f_i(a) \text{ si } a \in A_i,$$

es cota superior de $\mathcal{C}$. En efecto, es evidente que f está bien definida. Además es sobreyectiva ya que, dado $(a, b) \in A \times A$, existen índices $i, j \in I$ tales que $a \in A_i$ y $b \in A_j$. Podemos suponer que $(A_i, f_i) \preceq (A_j, f_j)$, luego $a, b \in A_j$ y, puesto que $f_j : A_j \to A_j \times A_j$ es sobreyectiva, existe $u \in A_j$ tal que $f_j(u) = (a, b)$. Por tanto, $u \in A$ y $f(u) = (a, b)$, lo que prueba la sobreyectividad de f.

Por otro lado, vemos que f es inyectiva pues, si $x, y \in A$ y $f(x) = f(y)$, existen $i, j \in I$ tales que $x \in A_i$ e $y \in A_j$. Podemos suponer que $(A_i, f_i) \preceq (A_j, f_j)$, luego $x, y \in A_j$ y $f_j(x) = f_j(y)$. Se deduce de la inyectividad de f_j que $x = y$.

Hemos probado que $(A, f) \in \Sigma$ y, de la definición, se deduce que $(A_i, f_i) \preceq (A, f), \forall i \in I$. Por el Lema de Zorn, existe un elemento maximal $(M, f) \in \Sigma$. Denotemos $N := X \backslash M$. Si $\mathrm{Card}(N) \leq \mathrm{Card}(M)$ entonces, por la Proposición III.1.5,

$$\mathrm{Card}(M) \leq \mathrm{Card}(X) = \mathrm{Card}(M \sqcup N) \leq \mathrm{Card}(M \times \{0, 1\}) = \mathrm{Card}(M),$$

luego, por el Teorema de Cantor-Bernstein, $\mathrm{Card}(M) = \mathrm{Card}(X)$.

Existe, por tanto, una biyección $h : X \to M$. También es biyectiva la aplicación

$$h \times h : X \times X \to M \times M, (x, y) \mapsto (h(x), h(y)),$$

luego

$$(h \times h)^{-1} \circ f \circ h : X \to X \times X$$

es biyectiva y hemos terminado en este caso.

Para concluir basta demostrar el caso que falta por estudiar, esto es, que $\mathrm{Card}(M) < \mathrm{Card}(N)$, el cual vemos que no puede darse.

En efecto, supongamos que $\mathrm{Card}(M) < \mathrm{Card}(N)$ y sea $\mathtt{j} : M \hookrightarrow N$ una aplicación inyectiva. Entonces $M_1 := \mathtt{j}(M) \subset N$ y $\mathrm{Card}(M_1) = \mathrm{Card}(M)$. Escribimos

$$(M \sqcup M_1) \times (M \sqcup M_1) = (M \times M) \sqcup (M \times M_1) \sqcup (M_1 \times M) \sqcup (M_1 \times M_1),$$

que es una unión disjunta porque $M_1 \subset N = X \setminus M$. Nótese que $M \subsetneq M \sqcup M_1$. Como $(M, f) \in \Sigma$ y $\mathrm{Card}(M_1) = \mathrm{Card}(M)$, se tiene

$$\mathrm{Card}(M_1 \times M) = \mathrm{Card}(M \times M_1) = \mathrm{Card}(M_1 \times M_1) = \mathrm{Card}(M \times M)$$

y se deduce que el conjunto

$$M_2 := (M_1 \times M) \sqcup (M \times M_1) \sqcup (M_1 \times M_1),$$

que es disjunto con $M \times M$, cumple $\mathrm{Card}(M_2) = \mathrm{Card}(M \times M) = \mathrm{Card}(M)$, donde las igualdades se deben a los apartados (3) y (2) de la Proposición III.1.5, respectivamente. En consecuencia, $\mathrm{Card}(M_1) = \mathrm{Card}(M) = \mathrm{Card}(M_2)$ y existen biyecciones $f : M \to M \times M$ y $g : M_1 \to M_2$. Definimos

$$G : M \sqcup M_1 \to (M \sqcup M_1) \times (M \sqcup M_1) = (M \times M) \sqcup M_2, x \mapsto \begin{cases} f(x) & \text{si } x \in M, \\ g(x) & \text{si } x \in M_1. \end{cases}$$

Observamos que esta aplicación está bien definida porque M y M_1 son disjuntos y es inyectiva por serlo $G|_M = f$ y $G|_{M_1} = g$ y ser $(M \times M) \cap M_2 = \varnothing$. Además vemos que es sobreyectiva. En efecto, dado $y \in (M \times M) \sqcup M_2$, o bien $y \in M \times M$ o bien $y \in M_2$. En el primer caso, por ser f sobreyectiva, existe un $x \in M$ tal que $G(x) = f(x) = y$ y, en el segundo caso, existe, por ser g sobreyectiva, un $x \in M_1$ tal que $G(x) = g(x) = y$.

Esto demuestra que el par $(M \sqcup M_1, G)$ pertenece a Σ pero $(M, f) \prec (M \sqcup M_1, G)$, lo que contradice la maximalidad de (M, f).

(2) Argumentamos por inducción sobre n, siendo obvio el caso $n = 1$. Sea $n > 1$ y supongamos ya probado que $\mathrm{Card}(X) = \mathrm{Card}(X^{n-1})$. Existe, por tanto, una biyección $f : X \to X^{n-1}$, luego $g : X \times X \to X^n, (x, y) \mapsto (f(x), y)$ es también biyectiva. Por el primer apartado existe una biyección $h : X \to X \times X$ y $g \circ h : X \to X^n$ es biyectiva. □

Corolario III.1.8. *Sea X un conjunto infinito. Entonces, existe una aplicación biyectiva $X \times \mathbb{N} \to X$.*

Demostración. Como la aplicación $X \hookrightarrow X \times \mathbb{N}, x \mapsto (x, 1)$ es inyectiva, es suficiente, por el Teorema de Cantor-Bernstein, demostrar que existe una aplicación inyectiva $X \times \mathbb{N} \hookrightarrow X$. Por el apartado (1) de la Proposición III.1.4, existe una aplicación inyectiva $\mathrm{j} : \mathbb{N} \hookrightarrow X$, por lo que la aplicación

$$f : X \times \mathbb{N} \hookrightarrow X \times X, (x, n) \mapsto (x, \mathrm{j}(n))$$

es, también, inyectiva.

En el primer apartado del Corolario III.1.7 hemos demostrado que existe una aplicación inyectiva $g : X \times X \hookrightarrow X$, por lo que la composición $g \circ f : X \times \mathbb{N} \hookrightarrow X$ es inyectiva y hemos terminado. □

Corolario III.1.9. *Sean X un conjunto infinito y $\{A_i : i \in I\}$ una familia de subconjuntos finitos, no vacíos y disjuntos de X. Suponemos que I es infinito. Entonces,*

$$\mathrm{Card}(\bigsqcup_{i\in I} A_i) = \mathrm{Card}(I).$$

Demostración. Por el axioma de elección podemos tomar un elemento $a_i \in A_i$ para cada $i \in I$. La aplicación

$$I \to \bigsqcup_{i\in I} A_i, k \mapsto a_k$$

está bien definida y es inyectiva porque los conjuntos A_i son disjuntos dos a dos. Por el Teorema de Cantor-Bernstein, para demostrar la igualdad del enunciado, es suficiente encontrar una aplicación inyectiva $\bigsqcup_{i\in I} A_i \hookrightarrow I$. Fijado $i \in I$, el conjunto A_i es finito, luego existe una aplicación inyectiva $f_i : A_i \hookrightarrow \mathbb{N}$. Entonces, la aplicación

$$g : \bigsqcup_{i\in I} A_i \hookrightarrow \mathbb{N} \times I, x \mapsto (f_i(x), i) \text{ si } x \in A_i$$

es también inyectiva. Por el apartado (1) de la Proposición III.1.4, existe una aplicación inyectiva $h : \mathbb{N} \hookrightarrow I$, así que también es inyectiva la aplicación

$$H : \mathbb{N} \times I \hookrightarrow I \times I, (n, i) \mapsto (h(n), i).$$

Por último, por el Corolario III.1.7, existe una biyección $F : I \times I \to I$ y, por ello, la composición

$$F \circ H \circ g : \bigsqcup_{i\in I} A_i \hookrightarrow I$$

es una aplicación inyectiva, como buscábamos. □

Antes de continuar la sección con los últimos resultados sobre cuerpos, vamos a demostrar que un conjunto que no sea finito es, en efecto, infinito. Este resultado se apoya en el Corolario III.1.9 y en el Axioma de elección. Observemos que, en la demostración, sólo sería necesario utilizar el *Axioma de elección numerable*, el cual permite tomar un elemento de cada conjunto de una colección numerable, que resulta ser una versión estrictamente más débil que el primero.

Proposición III.1.10. *Todo conjunto A no finito es infinito.*

Demostración. Comenzamos construyendo una aplicación $f : \mathbb{N} \to \mathcal{P}(\mathcal{P}(A))$ tal que para cada natural n, $f(n)$ es el conjunto formado por los subconjuntos finitos de A con cardinal n. Observamos que $f(n)$ no puede ser vacío. En caso contrario, existiría un n_0 tal que $f(n_0) = \varnothing$ y, por tanto, $\mathrm{Card}(A) \leq n_0 - 1$, por lo que A sería finito.

El conjunto $\mathrm{im}(f) := \{f(n) : n \in \mathbb{N}\}$ cumple que es un conjunto numerable cuyos elementos son conjuntos no finitos, posiblemente no numerables. Por el Axioma de elección, existe un conjunto $G := \{g(n) : n \in \mathbb{N}\}$ tal que, para cada $n \in \mathbb{N}$, $g(n)$ sea un miembro de $f(n)$ y, por tanto, un subconjunto finito de cardinal n.

Sea $\mathcal{U} := \bigcup_{n\in\mathbb{N}} g(n)$. Por el Corolario III.1.9, $\mathrm{Card}(\mathcal{U}) = \mathrm{Card}(\mathbb{N}) = \aleph_0$, luego existe una biyección $h : \mathbb{N} \to \mathcal{U}$. Definimos, finalmente, una biyección

$$F : A \to A \setminus h(0), x \mapsto \begin{cases} x & \text{si } x \in A \setminus \mathcal{U}, \\ h(n+1) & \text{si } x = h(n) \in \mathcal{U}, \end{cases}$$

por lo que A es infinito. □

Es conveniente observar que con este resultado, junto a la Proposición I.1.8, cualquier conjunto es finito o infinito. De esta manera, la Proposición I.1.9 se aplica a cualquier conjunto.

Lema III.1.11. *(1) Sean K un cuerpo infinito y $\aleph := \mathrm{Card}(K)$. Entonces, $\aleph$ es el cardinal del anillo de polinomios $K[\mathtt{t}]$.*

(2) Sean K un cuerpo y $\aleph := \max\{\mathrm{Card}(K), \aleph_0\}$. Entonces $\mathrm{Card}(K[\mathtt{t}]) = \aleph$.

Demostración. (1) Para cada $d \in \mathbb{N}$, sea $K_d[\mathtt{t}]$ el conjunto de los polinomios de $K[\mathtt{t}]$ de grado menor o igual que d, que es un K-espacio vectorial que tiene por base a $\mathcal{B}_d := \{1, \mathtt{t}, \ldots, \mathtt{t}^d\}$. Por tanto, $K_d[\mathtt{t}]$ es isomorfo, como K-espacio vectorial, a K^{d+1}, luego $\mathrm{Card}(K_d[\mathtt{t}]) = \mathrm{Card}(K)$ por el Corolario III.1.7(2).

Por otro lado, el cardinal del subconjunto $E_d \subset K_d[\mathtt{t}]$, formado por los polinomios de grado exactamente d, es el de K. En efecto, $\mathrm{Card}(E_d) \leq \mathrm{Card}(K^{d+1}) = \aleph$ por ser $E_d \subset K_d[\mathtt{t}]$. A su vez, la aplicación

$$(K \setminus \{0\}) \times K_{d-1}[\mathtt{t}] \to E_d, (a, f) \mapsto a\mathtt{t}^d + f$$

es inyectiva y $\mathrm{Card}(K \setminus \{0\}) = \mathrm{Card}(K_{d-1}[\mathtt{t}]) = \aleph$. Por el Corolario III.1.7,

$$\aleph = \mathrm{Card}((K \setminus \{0\}) \times K_{d-1}[\mathtt{t}]) \leq \mathrm{Card}(E_d)$$

y se deduce del Teorema de Cantor-Bernstein que $\mathrm{Card}(E_d) = \aleph$.

De esta manera, $K[\mathtt{t}] = \bigsqcup_{d\in\mathbb{N}} E_d$ es una unión disjunta de los conjuntos E_d, cada uno de los cuales tiene el cardinal de K. Por ello, el cardinal de $K[\mathtt{t}]$ es el de $K \times \mathbb{N}$, que es el de K, en virtud del Corolario III.1.8.

(2) Si K es infinito, tenemos que su cardinal es mayor o igual que $\aleph_0$ por la Proposición III.1.4, luego basta aplicar el primer apartado. En el caso de que K sea finito, entonces lo es cada $K_d[\mathtt{t}]$, luego

$$K[\mathtt{t}] = \bigsqcup_{d\in\mathbb{N}} E_d$$

es unión numerable y disjunta de conjuntos finitos. Se desprende del Corolario III.1.9 que $\mathrm{Card}(K[\mathtt{t}]) = \aleph_0 = \aleph$. □

Teorema III.1.12. *Todo cuerpo K admite un cierre algebraico.*

Demostración. Denotemos $\aleph_0 := \mathrm{Card}(\mathbb{N})$ y $\aleph := \max\{\mathrm{Card}(K), \aleph_0\}$. Escogemos un conjunto cualquiera S que contenga a K y cuyo cardinal sea mayor que $\aleph$; por ejemplo, $S := \mathcal{P}(K) \times \mathbb{R}$ pues $\mathrm{Card}(K) < \mathrm{Card}(\mathcal{P}(K))$, según vimos en la Proposición I.1.9. Además, la aplicación $\mathtt{j} : K \hookrightarrow \mathcal{P}(K) \times \mathbb{R}, x \mapsto (\{x\}, 0)$ es inyectiva e identificamos K con $\mathtt{j}(K) \subset S$.

Veamos que *si $L|K$ es una extensión algebraica de K, entonces existe una aplicación inyectiva $\mathtt{j} : L \hookrightarrow S$ tal que $\mathtt{j}|_K = id_K$*. En efecto, como las preimágenes de la aplicación $L \to K[\mathtt{t}], a \mapsto P_{K,a}$ tienen cardinal finito y vimos en el Lema III.1.11 que $\mathrm{Card}(K[\mathtt{t}]) = \aleph$, se sigue del Corolario III.1.9 que $\mathrm{Card}(L) = \aleph$. En particular, deducimos del Corolario III.1.6 que

$$\mathrm{Card}(L \setminus K) \leq \mathrm{Card}(L) = \aleph < \mathrm{Card}(S) = \mathrm{Card}(S \setminus K).$$

Para construir una aplicación inyectiva $\mathtt{j} : L \hookrightarrow S$ tal que $\mathtt{j}|_K = \mathrm{id}_K$ basta elegir una aplicación inyectiva $\mathtt{j}' : L \setminus K \hookrightarrow S \setminus K$ y definir

$$\mathtt{j} : L \hookrightarrow S, x \mapsto \begin{cases} x & \text{si } x \in K, \\ \mathtt{j}'(x) & \text{si } x \in L \setminus K. \end{cases}$$

Consideramos la familia Σ formada por todos los pares $(L, \mathtt{j})$ donde $L|K$ es una extensión algebraica de K y $\mathtt{j} : L \hookrightarrow S$ es una aplicación inyectiva tal que $\mathtt{j}|_K = \mathrm{id}_K$. Sea $\mathtt{i} : K \hookrightarrow S$ la aplicación inyectiva inducida por la inclusión $K \subset S$. Como $(K, \mathtt{i}) \in \Sigma$, este conjunto es no vacío. Observamos además que $\mathtt{j}(1_L) = \mathtt{j}(1_K) = 1_K$ para cada $(L, \mathtt{j}) \in \Sigma$.

Definimos en Σ la siguiente relación de orden: dados $(L_1, \mathtt{j}_1), (L_2, \mathtt{j}_2) \in \Sigma$ diremos que $(L_1, \mathtt{j}_1) \preceq (L_2, \mathtt{j}_2)$ si $L_2|L_1$ (abusando de la notación escribiremos $L_1 \subset L_2$) y $\mathtt{j}_2|_{L_1} = \mathtt{j}_1$. Veamos que el par $(\Sigma, \preceq)$ es inductivo.

Denotemos $\Lambda := \{(L_i, \mathtt{j}_i)\}_{i \in I} \subset \Sigma$ un subconjunto totalmente ordenado. Observemos primero que si $(L_1, \mathtt{j}_1) \preceq (L_2, \mathtt{j}_2)$, entonces $\mathtt{j}_1(L_1) \subset \mathtt{j}_2(L_2)$. Definimos $L := \bigcup_{i \in I} \mathtt{j}_i(L_i)$ al que vamos a dotar de estructura de cuerpo. Como Λ es un conjunto totalmente ordenado, dados $x, y \in L$ existe $i \in I$ tales que $x, y \in \mathtt{j}_i(L_i)$. Definimos las operaciones

$$x + y := \mathtt{j}_i(\mathtt{j}_i^{-1}(x) + \mathtt{j}_i^{-1}(y)),$$
$$x \cdot y := \mathtt{j}_i(\mathtt{j}_i^{-1}(x) \cdot \mathtt{j}_i^{-1}(y)).$$

Las relaciones de compatibilidad $L_i \subset L_k$ y $\mathtt{j}_k|_{L_i} = \mathtt{j}_i$ si $(L_i, \mathtt{j}_i) \preceq (L_k, \mathtt{j}_k)$ garantizan que las operaciones anteriores están bien definidas y dotan a L de estructura de anillo. De hecho, es un cuerpo, ya que para cada $x \in \mathtt{j}_i(L_i) \subset L$ existe $u \in L_i$ tal que $x = \mathtt{j}_i(u)$ y, si $u^{-1} \in L_i$ es el inverso de u, entonces $\mathtt{j}_i(u^{-1}) \in \mathtt{j}_i(L_i) \subset L$ es el inverso de x, pues

$$x \cdot \mathtt{j}_i(u^{-1}) = \mathtt{j}_i(\mathtt{j}_i^{-1}(x) \cdot \mathtt{j}_i^{-1}\mathtt{j}_i(u^{-1})) = \mathtt{j}_i(u \cdot u^{-1}) = \mathtt{j}_i(1_{L_i}) = 1_K.$$

De la construcción (y abusando de la notación) se desprende que $L|L_i$ es una extensión de cuerpos y podemos escribir $L_i \subset L$ (abusando un poco más). Consideramos la aplicación

inyectiva $\mathtt{j}_L : L \hookrightarrow S$ inducida por la inclusión $L \subset S$ y resulta inmediato comprobar que $(L, \mathtt{j}_L) \in \Sigma$ es una cota superior de Λ en Σ.

Lo anterior implica, por el Lema de Zorn, que el conjunto Σ posee un elemento maximal, que denotamos $(L_0, \mathtt{j}_0)$, y vamos a probar que es un cierre algebraico de K. Como $L_0 \in \Sigma$, la extensión $L_0|K$ es algebraica, luego todo consiste en demostrar que L_0 es un cuerpo algebraicamente cerrado. En caso contrario existiría un polinomio irreducible $f \in L_0[\mathtt{t}]$ de grado mayor o igual que 1 que no tiene ninguna raíz en L_0. Ahora bien, el cuerpo $E := L_0[\mathtt{t}]/fL_0[\mathtt{t}]$ es una extensión de grado $\deg(f)$ de L_0, luego es extensión algebraica y $u := \mathtt{t} + fL_0[\mathtt{t}]$ es una raíz de f. Como las extensiones $E|L_0$ y $L_0|K$ son algebraicas, también lo es $E|K$. Esto implica, por lo probado al comenzar el segundo párrafo de la demostración del teorema, que $\mathrm{Card}(E) = \aleph$ y, como $\aleph < \mathrm{Card}(S)$, se deduce, de nuevo por el Corolario III.1.6 y puesto que $\mathrm{Card}(\mathtt{j}(L_0)) = \mathrm{Card}(L_0) < \mathrm{Card}(S)$, que

$$\mathrm{Card}(E \setminus L_0) \leq \mathrm{Card}(E) = \aleph < \mathrm{Card}(S) = \mathrm{Card}(S \setminus \mathtt{j}(L_0)).$$

Veamos ahora que existe una aplicación inyectiva $\mathtt{j} : E \hookrightarrow S$ cuya restricción a L_0 es $\mathtt{j}_0$.

Para construirla, elegimos una aplicación inyectiva $\mathtt{j}_1 : E \setminus L_0 \hookrightarrow S \setminus \mathtt{j}(L_0)$ y definimos

$$\mathtt{j} : E \hookrightarrow S, x \mapsto \begin{cases} \mathtt{j}_0(x) & \text{si } x \in L_0, \\ \mathtt{j}_1(x) & \text{si } x \in E \setminus L_0. \end{cases}$$

De esta manera, $(L_0, \mathtt{j}_0) \prec (E, \mathtt{j})$, lo que contradice la maximalidad de $(L_0, \mathtt{j}_0)$. Así, L_0 es un cuerpo algebraicamente cerrado, como queríamos. □

Lema III.1.13. *Sea* $\mathtt{j} : K_1 \to K_2$ *un homomorfismo de cuerpos de modo que* K_2 *es algebraicamente cerrado y sea* $L|K_1$ *una extensión algebraica. Entonces, existe un homomorfismo* $\psi : L \to K_2$ *tal que* $\psi|_{K_1} = \mathtt{j}$.

Demostración. Sea Σ el conjunto de todos los pares (F, φ), donde $F|K_1$ es una subextensión de $L|K_1$ y $\varphi : F \to K_2$ es un homomorfismo tal que $\varphi|_{K_1} = \mathtt{j}$. El conjunto Σ es no vacío ya que el par $(K_1, \mathtt{j}) \in \Sigma$ y definimos en Σ el orden

$$(F_1, \varphi_1) \preceq (F_2, \varphi_2) \text{ si } F_1 \subset F_2 \text{ y } \varphi_2|_{F_1} = \varphi_1.$$

Vamos a utilizar el Lema de Zorn para probar que Σ contiene un elemento maximal. Para ello consideramos una cadena cualquiera $\mathcal{C} := \{(F_i, \varphi_i)\}_{i \in I}$ de Σ. Observamos que, por tratarse de un subconjunto totalmente ordenado, la unión $F := \bigcup_{i \in I} F_i$ es un cuerpo y $F|K_1$ es subextensión de $L|K_1$ por serlo cada $F_i|K$. Además, la aplicación

$$\varphi : F \to K_2, x \mapsto \varphi_i(x) \text{ si } x \in F_i$$

está bien definida pues, si $x \in F_i \cap F_j$, podemos suponer que $(F_i, \varphi_i) \preceq (F_j, \varphi_j)$, por ser $\mathcal{C}$ totalmente ordenado, y $\varphi_i(x) = \varphi_j(x)$. De hecho, φ es homomorfismo pues, dados

$x, y \in F$, existen $i, j \in I$ tales que $x \in F_i$ e $y \in F_j$ y, de nuevo, podemos suponer que $(F_i, \varphi_i) \preceq (F_j, \varphi_j)$. Por tanto,

$$\varphi(x+y) = \varphi_j(x+y) = \varphi_j(x) + \varphi_j(y) = \varphi(x) + \varphi(y)$$

$$\varphi(x \cdot y) = \varphi_j(x \cdot y) = \varphi_j(x) \cdot \varphi_j(y) = \varphi(x) \cdot \varphi(y).$$

Nótese que $\varphi|_{K_1} = \mathtt{j}$, luego el par (F, φ) pertenece a Σ y $(F_i, \varphi_i) \preceq (F, \varphi)$ para cada $i \in I$, por lo que tenemos que $(F, \varphi) \in \Sigma$ es cota superior de $\mathcal{C}$. Por el Lema de Zorn, existe un elemento maximal (E, ψ) y nos basta probar que $E = L$. Desde luego, $E|K_1$ es subextensión de $L|K_1$ y, si $E \subsetneq L$, existe $\alpha \in L \setminus E$. Este elemento es algebraico sobre K_1, luego es algebraico sobre E. Si denotamos

$$f_1(\mathtt{t}) := P_{E,\alpha} = \mathtt{t}^m + \sum_{k=0}^{m-1} a_k t^k$$

y definimos $f_2(\mathtt{t}) := \mathtt{t}^m + \sum_{k=0}^{m-1} \psi(a_k)\mathtt{t}^k \in K_2[\mathtt{t}]$, el cual sabemos que tiene alguna raíz $\beta \in K_2$ por ser éste algebraicamente cerrado. De esta manera y denotando $E(\alpha)$, existe un homomorfismo

$$\widehat{\psi} : E(\alpha) \to K_2, \sum_{i=0}^{m-1} b_i \alpha^i \mapsto \sum_{i=0}^{m-1} \psi(b_i)\beta^i$$

tal que $\widehat{\psi}(\alpha) = \beta$ y $\widehat{\psi}|_E = \psi$, luego $(E(\alpha), \widehat{\psi}) \in \Sigma$ y $(E, \psi) \prec (E(\alpha), \widehat{\psi})$, contra la maximalidad de (E, ψ) en Σ. Por tanto, $L = E$ y hemos acabado. □

Teorema III.1.14. *Dados dos cierres algebraicos $(K, \mathtt{j}_1, L_1)$ y $(K, \mathtt{j}_2, L_2)$ de un cuerpo K, existe un isomorfismo de cuerpos $\varphi : L_1 \to L_2$ tal que $\mathtt{j}_2 = \varphi \circ \mathtt{j}_1$.*

Demostración. Como la extensión $L_1|K$ es algebraica y $\mathtt{j}_2 : K \to L_2$ es un homomorfismo, existe, por el lema anterior y por ser L_2 algebraicamente cerrado, un homomorfismo $\varphi : L_1 \to L_2$ tal que $\varphi \circ \mathtt{j}_1 = \mathtt{j}_2$. En particular, $L_1 \simeq \varphi(L_1) \subset L_2$. Como L_1 es algebraicamente cerrado, también lo es $\varphi(L_1)$, que contiene a $\varphi(\mathtt{j}_1(K)) = \mathtt{j}_2(K)$. Por esto último y dado que la extensión $L_2|K$ es algebraica, también lo es $L_2|\varphi(L_1)$ luego, por la Proposición III.1.1, la extensión ha de ser trivial y $\varphi(L_1) = L_2$. Por tanto, $\varphi : L_1 \to L_2$ es un isomorfismo que cumple $\mathtt{j}_2 = \varphi \circ \mathtt{j}_1$. □

III.2. Existencia y equicardinalidad de las bases de un espacio vectorial

Comenzamos recordando las nociones básicas acerca de la dependencia lineal en espacios vectoriales.

Definición III.2.1. Sean K un cuerpo, V un K-espacio vectorial no nulo y X un subconjunto no vacío de V.

(1) Se dice que X es *ligado* si existen $v_1, \ldots, v_n \in X$ y $a_1, \ldots, a_n \in K$, no todos nulos, tales que $a_1 v_1 + \cdots + a_n v_n = 0_V$. Si X no es ligado, se denomina *libre.*

(2) Se llama *subespacio vectorial generado por* X, y se denota $\mathcal{L}[X]$, al conjunto formado por las *combinaciones lineales* de vectores de X, es decir, todos los vectores de la forma $a_1 v_1 + \cdots + a_n v_n$ donde $a_i \in K, v_i \in X, \forall i = 1, \ldots, n$.

(3) Se dice que X es una *base* de V si es libre y un *sistema generador* de V, es decir, $V = \mathcal{L}[X]$.

Observación III.2.2. (1) Todo subconjunto de V que contiene a uno ligado es también ligado. De la misma manera, todo subconjunto no vacío de uno libre es también libre. Además, se deduce de las definición que X es libre si, y sólo si, lo son todos sus subconjuntos finitos. En efecto, si hubiese un subconjunto finito ligado, lo sería también el total. Por otra parte, si X es ligado, existen $v_1, \ldots, v_n \in X$ y $a_1, \ldots, a_n \in K$ tales que $a_1 v_1 + \cdots + a_n v_n = 0_V$, luego $S := \{v_1, \ldots, v_n\}$ es un subconjunto ligado y finito de X.

(2) Sean $X \subset V$ libre y $v \in V \setminus \mathcal{L}[X]$. Entonces $Y := X \cup \{v\}$ es también libre. En efecto, en caso contrario existirían vectores $v_1, \ldots, v_n \in X$ y $a, a_1, \ldots, a_n \in K$ tales que la tupla $(a, a_1, \ldots, a_n)$ no es nula y $av + a_1 v_1 + \cdots + a_n v_n = 0_V$. Como X es libre, tenemos que $a \neq 0$ y, denotando $b_i := \frac{-a_i}{a}$ para $i = 1, \ldots, n$, resulta $v = b_1 v_1 + \cdots + b_n v_n \in \mathcal{L}[X]$, que es falso.

Proposición III.2.3. *Todo K-espacio vectorial no nulo posee una base.*

Demostración. Denotamos Γ el conjunto formado por todos los subconjuntos libres del K-espacio vectorial no nulo V. Vemos que no es vacío ya que, si $v \in V \setminus \{0_V\}$, entonces el conjunto $\{v\}$ es libre. Definimos en Γ la relación de orden dada por la inclusión y observamos que si $\mathcal{C} := \{X_i : i \in I\}$ es una cadena en Γ, entonces $X := \bigcup_{i \in I} X_i$ pertenece a Γ. En efecto, se trata de probar que X es libre y, en virtud de la Observación III.2.2(1), basta ver que lo es cualquier subconjunto finito de X. Esto es obvio pues, al ser $\mathcal{C}$ totalmente ordenado, los subconjuntos finitos de X lo son de algún X_i, que es libre por hipótesis. Concluimos que X es cota superior de $\mathcal{C}$. Por el Lema de Zorn existe un elemento maximal $\mathcal{B}$ de Γ y veamos que se trata de una base de V o, lo que es lo mismo, que genera V. En caso contrario existiría un $v \in V \setminus \mathcal{L}[\mathcal{B}]$ lo que, por la Observación III.2.2, implica que $\mathcal{B} \cup \{v\}$ es libre, contradiciendo la maximalidad de $\mathcal{B}$ en Γ. □

Lema III.2.4. *Sean V un K-espacio vectorial no nulo, $X_1 \subset V$ un subconjunto libre y X_2 un sistema generador de V. Supongamos que X_1 y X_2 son finitos. Entonces* $\mathrm{Card}(X_1) \leq \mathrm{Card}(X_2)$.

Demostración. Escribimos

$$X_1 := \{u_1, \ldots, u_m\} \text{ y } X_2 := \{v_1, \ldots, v_n\}.$$

Como $u_1 \in V = \mathcal{L}[X_2]$, existen $a_1, \ldots, a_n \in K$ no todos nulos (ya que $u_1 \neq 0_V$ por ser X_1 libre) tales que $u_1 = a_1 v_1 + \cdots + a_n v_n$. Reordenando los vectores de X_2 si es preciso, podemos suponer que $a_1 \neq 0$, luego $v_1 \in \mathcal{L}[Y_1]$, donde $Y_1 := \{u_1, v_2, \ldots, v_n\}$. Como $\{u_1, v_1, \ldots, v_n\}$ es un sistema generador de V y $v_1 \in \mathcal{L}[Y_1]$, concluimos que Y_1 es un sistema generador de V. Supongamos que hemos repetido el proceso t veces y consideramos el conjunto generador $Y_t := \{u_1, \ldots, u_t, v_{t+1}, \ldots, v_n\}$. Vemos que el elemento u_{t+1} puede escribirse como $u_{t+1} := \sum_{i=0}^{t} a_i u_i + \sum_{i=t+1}^{n} b_i v_i$ donde no todos los b_i son nulos pues, en caso contrario, X_1 no sería libre. De la manera anterior, podemos construir el conjunto $Y_{t+1} := \{u_1, \ldots, u_{t+1}, \ldots, v_{t+2}, \ldots, v_n\}$.

Consideramos ahora el sistema generador $Y_m := \{u_1, \ldots, u_m, \ldots, v_{m+1}, \ldots, v_n\}$ donde $n - m = k$ para cierto entero $k \geq 0$. Así,

$$\mathrm{Card}(X_1) = m \leq m + k = n = \mathrm{Card}(X_2).$$

□

Teorema III.2.5. *Sean V un K-espacio vectorial no nulo y $\mathcal{B}_1, \mathcal{B}_2$ dos bases de V. Entonces* $\mathrm{Card}(\mathcal{B}_1) = \mathrm{Card}(\mathcal{B}_2)$.

Demostración. Supongamos que no se cumple la igualdad. Por el Principio de comparación de cardinales introducido en la Sección II.2, podemos suponer que $\mathrm{Card}(\mathcal{B}_1) < \mathrm{Card}(\mathcal{B}_2)$. Si $\mathcal{B}_2$ es un conjunto finito, también lo es $\mathcal{B}_1$. Como $\mathcal{B}_2$ es libre y $\mathcal{B}_1$ es sistema generador, se deduce del Lema III.2.4 que $\mathrm{Card}(\mathcal{B}_2) \leq \mathrm{Card}(\mathcal{B}_1)$, lo que es una contradicción.

Suponemos, por tanto, que $\mathcal{B}_2$ es un conjunto infinito y escribimos

$$\mathcal{B}_1 := \{u_i : i \in I\} \text{ y } \mathcal{B}_2 := \{v_j : j \in J\}.$$

Para cada $i \in I$ existen un subconjunto finito $E_i \subset J$ y escalares $\lambda_{ij} \in K$ tales que

$$u_i := \sum_{j \in E_i} \lambda_{ij} v_j.$$

Por el Corolario III.1.9, $\mathrm{Card}(\bigcup_{i \in I} E_i) = \mathrm{Card}(I) < \mathrm{Card}(J)$, luego $\bigcup_{i \in I} E_i \subsetneq J$ y elegimos $j_0 \in J \setminus \bigcup_{i \in I} E_i$. Como $v_{j_0} \in V = \mathcal{L}[\mathcal{B}_1]$, existen un subconjunto finito $F := \{i_1, \ldots, i_r\} \subset I$ y escalares $c_1, \ldots, c_r \in K$ tales que

$$v_{j_0} = \sum_{k=1}^{r} c_k u_{i_k} = \sum_{k=1}^{r} c_k \sum_{j \in E_{i_k}} \lambda_{i_k} v_j = \sum_{k=1,\ldots,r, j \in E_{i_k}} c_k \lambda_{i_k} v_j,$$

pero esto es absurdo ya que $\mathcal{B}_{\in}$ es libre y $v_{j_0} \in \mathcal{B}_2$. □

III.3. Existencia de ideales maximales en anillos conmutativos y unitarios

Empezamos recordando una serie de definiciones.

Definición III.3.1. (1) Un anillo $(A, +, \cdot)$ se dice *conmutativo* si para todo $a, b \in A$ se cumple $ab = ba$.

(2) Dícese que un anillo $(A, +, \cdot)$ es *unitario* si existe $1_A \in A$ tal que $a \cdot 1_A = 1_A \cdot a = a$ para cualquier $a \in A$.

(3) Se denominan *unidades* del anillo unitario $(A, +, \cdot)$ a los elementos $u \in A$ tales que existe $v \in A$ que cumple $uv = 1_A$. Se denota $\mathcal{U}(A)$ al conjunto formado por las unidades del anillo A.

(4) Se dice que un subconjunto $\mathfrak{a} \subset A$, donde A es conmutativo, es un *ideal* de A si es un subgrupo del grupo aditivo $(A, +)$ y $ax \in \mathfrak{a}$ para todo $(a, x) \in A \times \mathfrak{a}$. El propio anillo A es un ideal de A, llamado *ideal impropio*. Los restantes ideales de A se denominan *ideales propios*.

(5) Un ideal $\mathfrak{m}$ de A se dice *maximal* si no existe ningún ideal propio $\mathfrak{n}$ de A tal que $\mathfrak{m} \subsetneq \mathfrak{n}$.

Observación III.3.2. Un ideal $\mathfrak{a}$ de A es propio si y sólo si $\mathfrak{a} \cap \mathcal{U}(A) = \varnothing$. En efecto, si existiese $u \in \mathfrak{a} \cap \mathcal{U}(A)$, entonces existiría también $v \in A$ tal que $vu = 1_A$ y esto implicaría que, $\forall x \in A$,

$$x = x \cdot 1_A = x \cdot (vu) = (xv) \cdot u \in \mathfrak{a}.$$

Se concluye este trabajo demostrando la existencia de ideales maximales en los anillos conmutativos y unitarios.

Proposición III.3.3. *Sea A un anillo conmutativo y unitario. Se tiene:*

(1) Sea $\mathfrak{a} \subset A$ un ideal propio. Entonces existe un ideal maximal $\mathfrak{m}$ de A que contiene a $\mathfrak{a}$.

(2) A posee algún ideal maximal.

(3) Para cada $x \in A \setminus \mathcal{U}(A)$, existe un ideal maximal $\mathfrak{m} \subset A$ tal que $x \in \mathfrak{m}$.

(4) Para cada subconjunto $S \subset A$, o bien existe un ideal maximal que contiene a S, o bien el ideal $\langle S \rangle$ es A.

Demostración. (1) La familia de ideales

$$\mathcal{F} := \{\mathfrak{b} \subsetneq A \text{ ideal de } A : \mathfrak{a} \subset \mathfrak{b}\}$$

no es vacía, pues contiene al ideal $\mathfrak{a}$, y está parcialmente ordenada respecto a la inclusión conjuntista habitual.

Por otra parte, todo subconjunto totalmente ordenado $\mathcal{C} := \{\mathfrak{b}_i\}_{i\in I} \subset \mathcal{F}$ está acotado superiormente ya que $\mathfrak{b} = \bigcup_{i\in I} \mathfrak{b}_i \in \mathcal{F}$ es una cota superior suya. Por el Lema de Zorn, existe un elemento maximal $\mathfrak{m} \in \mathcal{F}$. Veamos que $\mathfrak{m}$ es un ideal maximal de A que contiene al ideal $\mathfrak{a}$.

Evidentemente $\mathfrak{a} \subset \mathfrak{m}$ ya que $\mathfrak{m} \in \mathcal{F}$. Por otro lado, si $\mathfrak{m}$ no fuese maximal, existiría un ideal $\mathfrak{n} \subsetneq A$ tal que $\mathfrak{m} \subsetneq \mathfrak{n}$. Pero entonces $\mathfrak{a} \subset \mathfrak{m} \subsetneq \mathfrak{n} \subsetneq A$ y, por tanto, $\mathfrak{n} \in \mathcal{F}$. Esto contradice la maximalidad de $\mathfrak{m}$ como elemento de $\mathcal{F}$ y hemos terminado.

(2) Basta aplicar el apartado anterior al ideal $\mathfrak{a} := \{0\}$.

(3) Como x no es unidad, el ideal principal xA no es A, luego por el primer apartado existe un ideal maximal $\mathfrak{m} \subset A$ que contiene a xA, así que $x \in \mathfrak{m}$.

(4) Si $\langle S\rangle$ no es el total, basta aplicar el primer apartado a dicho ideal para obtener un ideal maximal $\mathfrak{m}$ tal que $\langle S\rangle \subset \mathfrak{m}$ y, así, $S \subset \langle S\rangle \subset \mathfrak{m}$. □

Bibliografía

K. Conrad. Zorn's lemma and some applications i and ii. URL `https://kconrad.math.uconn.edu/blurbs/zorn1.pdf`. PDF en la red.

J.M. Gamboa and Beatriz Graña. *Álgebra Multilineal*. Editorial Sanz y Torres, 2021. ISBN 978-84-18316-20-3.

T. Jech. *Set Theory*. Springer Monographs, 1978.