

Álgebra I

Curso 2020/21

Índice

1	El lenguaje de los conjuntos	5
1.1	Sobre la teoría axiomática de conjuntos	6
1.1.1	Proposiciones y Demostraciones.	11
1.2	El conjunto producto cartesiano. Aplicaciones	15
1.2.1	Imágenes directas e inversas	18
1.3	Relaciones de equivalencia. Conjuntos cocientes.	21
2	Anillos conmutativos	25
2.1	Los anillos \mathbb{Z}_n	26
2.2	Generalidades	28
2.3	Los anillos de enteros cuadráticos $\mathbb{Z}[\sqrt{n}]$	30
2.4	Múltiplos y potencias naturales	32
2.5	Unidades. Cuerpos	33
2.6	Múltiplos negativos y potencias de exponente negativo	35
2.7	Los anillos de polinomios $A[x]$	37
2.8	Homomorfismos	40
3	Divisibilidad en Dominios Euclideos	43
3.1	Dominios de Integridad	43
3.2	El cuerpo de fracciones de un DI	44
3.3	Divisibilidad	46
3.4	Dominios Euclideos	48
3.5	Máximo común divisor	52
3.6	Ecuaciones diofánticas	56
3.7	Mínimo común múltiplo	58
3.8	Congruencias	59
3.9	La ecuación básica $ax \equiv b \pmod{m}$	61
3.10	Sistemas de congruencias	62
3.10.1	Sistemas de 2 congruencias	62
3.10.2	Sistemas de r congruencias	63
4	Anillos cocientes	65
4.1	Complementos sobre \mathbb{Z}_n	66
4.1.1	La ecuación $ax = b$ en \mathbb{Z}_n	66
4.1.2	La función φ de Euler	67

5	Dominios de Factorización Única	73
5.1	Caracterización de DFU	74
5.2	Todo DE es un DFU	75
5.3	Irreducibles y primos en $\mathbb{Z}[\sqrt{n}]$	76
5.4	Factorización única en anillos de polinomios	78
5.4.1	Criterios básicos de irreducibilidad de polinomios	81

Chapter 1

El lenguaje de los conjuntos

Comenzamos el curso con una breve discusión de las nociones de teoría de conjuntos que jugarán un papel esencial en vuestra formación matemática.

Su uso hoy día es fundamental para expresar de manera correcta los razonamientos y conceptos matemáticos.

Fue Georg Ferdinand Ludwig Philipp Cantor (San Petersburgo, 1845 -1918) quien expuso originalmente la Teoría de Conjuntos, sobre la que David Hilbert (Königsberg, Prusia Oriental, 1862-1943) declara

“Cantor ha creado para los matemáticos un paraíso de pensamiento del cual ya nadie nos expulsará”.

Al tiempo, fijaremos el sentido de los símbolos matemáticos básicos, que seguro os son ya familiares: \in (pertenece), \forall (para todo), \exists (existe), $|$ (tal que), \vee (o), \wedge (y), etc.

1.1 Sobre la teoría axiomática de conjuntos

La matemática es una ciencia totalmente abstracta. En contraposición con otras ciencias como pueden ser la física, la química o la biología, en matemáticas no hay forma de comprobar si un resultado es o no correcto. Esto hace que para realizar las matemáticas se establezca un contexto y en este contexto los matemáticos se pongan de acuerdo en que reglas o conceptos se dan por válidos.

Cantor propuso el contexto de “conjuntos” como el contexto básico en el que se establecen los axiomas y en el que se ha de desarrollar la matemática.

En el contexto de conjuntos hay dos nociones básicas:

- *Conjunto.*
- *Pertenece.*

Estas nociones básicas no se pueden definir pero si se deben entender. Además si aceptamos el contexto de conjuntos como aquel en el que vamos a desarrollar las matemáticas, sólo podremos hablar de conjuntos. Esto es: *Todo objeto matemático es un conjunto y cualquier enunciado debe estar basado en conjuntos y en la pertenencia.*

Una vez establecido el contexto en el que vamos a desarrollar las matemáticas, al ser esta una ciencia totalmente abstracta, necesitaremos establecer unas “reglas del juego” que nos permitan realizar nuestra ciencia.

Estas *reglas del juego* se conocen con el nombre de **Axiomas** y no tienen porqué ser aceptadas o estar fijadas de antemano. Los matemáticos tenemos que ponernos de acuerdo en los axiomas que vamos a aceptar. La única condición para aceptar estos axiomas será que **no den lugar a contradicciones**.

Los matemáticos Ernst Friedrich Ferdinand Zermelo (Berlín, 1871-1953) y Abraham Halevi Fraenkel (Múnich 1891-1965) fijaron la axiomática más aceptada de teoría de conjuntos: *La axiomática de Zermelo-Fraenkel*.

Utilizaremos cualquier tipo de letra,

$$A, B, C, \dots, X, Y, Z, \dots a, b, c, \dots, x, y, z, \dots, \alpha, \beta, \gamma, \dots$$

para expresar un conjunto.

Utilizaremos \in para indicar pertenece. Así escribiremos por ejemplo:

$$\text{Sea } x \in X.$$

Cuyo significado será:

$$\text{Sea } x \text{ un elemento de } X.$$

Y, por supuesto, tanto x como X , son conjuntos.

Comenzamos estableciendo un primer concepto: **El concepto de contenido:**

$$\text{Diremos que el conjunto } X \text{ está contenido en el conjunto } Y, \text{ y lo indicaremos } X \subseteq Y \text{ si todo elemento que pertenece a } X \text{ también pertenece a } Y.$$

Simbólicamente escribiremos:

Definición 1.1.1. $X \subseteq Y \Leftrightarrow \forall x \in X, x \in Y$.

El concepto de contenido está perfectamente definido. No como ocurre con el concepto de pertenece, que es básico y espero entendáis aunque no lo hemos (no podemos) definido.

El segundo concepto que definimos es el de igualdad. Simbólicamente:

Definición 1.1.2. $X = Y \Leftrightarrow X \subseteq Y \wedge Y \subseteq X$.

Que leeremos: X es igual a Y si (y solo si) X está contenido en Y e Y está contenido en X .

Ya que estamos hablando de un concepto (el de conjunto) totalmente abstracto, no podemos probar la existencia de ningún conjunto. Con el primer axioma aceptaremos la existencia de un conjunto especial, aquel que no tiene elementos:

Axioma 1: $\exists X; \forall x, x \notin X$.

Hasta ahora tenemos dos definiciones (contenido e igualdad) y un axioma, con esto podemos dar nuestro primer teorema:

Teorema 1.1.3. *Si X es un conjunto que satisface el Axioma 1, entonces $X \subseteq Y$, para cualquier conjunto Y .*

La demostración de este axioma es algo especial y no siempre este tipo de demostraciones fue aceptado. Es una demostración *por reducción al absurdo*. Este tipo de demostraciones consiste en negar la hipótesis del teorema y llegar a una contradicción, es decir hemos de llegar a algo que contradiga nuestros axiomas (en nuestro caso sólo tenemos el Axioma 1).

Lo primero que tenemos que saber es negar las hipótesis del Teorema 1.1.3.

Notemos que negar un enunciado del tipo:

$\forall Y$ se cumple bla, bla, bla.

Sería:

$\exists Y$ que no cumple bla, bla, bla.

Por tanto la negación de la hipótesis del Teorema 1.1.3 sería:

Si X es un conjunto que satisface el Axioma 1, entonces $\exists Y$ tal que $X \not\subseteq Y$.

Y la afirmación $X \not\subseteq Y$ nos diría que ha de existir un elemento $x \in X$ que no esté en Y . Lo que contradice la hipótesis de que X satisface el Axioma 1, ya que X no tiene elementos.

Una consecuencia (o corolario) inmediato de este Teorema 1.1.3 es que sólo existe un conjunto que satisfaga el Axioma 1. Que podemos enunciar como:

Corolario 1.1.4. *Existe un único conjunto que satisface el Axioma 1. Denotaremos a este conjunto como \emptyset o también 0 y lo llamaremos conjunto vacío o cero.*

Demostración. Si X_1 y X_2 son dos conjuntos que satisfacen el Axioma 1. Como X_1 satisface el Axioma 1 el Teorema 1.1.3 implica $X_1 \subseteq X_2$. Por otro lado como X_2 también satisface el Axioma 1, el mismo teorema nos daría $X_2 \subseteq X_1$. De donde tenemos la igualdad. ■

Hacer un estudio profundo de la axiomática de conjuntos en estos momentos sería muy arriesgado, habría muchas posibilidades de que no entenderíamos mucho y por otro lado este no es el objetivo del curso. Vamos entonces algunas reglas (de forma intuitiva) que me permitan trabajar o construir conjuntos, estas reglas están totalmente formalizadas en los axiomas de Zermelo-Fraenkel.

¿Cómo podemos dar un conjunto?

La axiomática nos permite dar un conjunto de dos formas distintas:

- Por extensión.
- Por comprensión.

Daremos un conjunto X por **extensión** cuando especifiquemos todos los elementos de X . Por ejemplo, si ya conocemos otros conjuntos a, b, c , podremos dar un nuevo conjunto cuyos elementos son estos tres conjuntos. Indicaremos esto como:

$$X = \{a, b, c\}.$$

A partir del único conjunto que tenemos hasta ahora, el vacío \emptyset o cero 0 , podemos dar (por extensión) un nuevo conjunto:

$$1 = \{\emptyset\} = \{0\}.$$

Este conjunto tiene un sólo elemento que es el conjunto vacío. Ya disponemos de dos conjuntos \emptyset y 1 y por tanto podemos dar (por extensión) otro nuevo conjunto, el que tiene a estos dos como elementos:

$$2 = \{0, 1\}.$$

Podemos ya construir infinitos conjuntos: $3 = \{0, 1, 2\}, 4 = \{0, 1, 2, 3\}, \dots$

Sin embargo, **NO** podemos dar por extensión el conjunto

$$\mathbb{N} = \{0, 1, 2, 3, \dots\},$$

Dar un conjunto por extensión significa dar o listar “*todos sus elementos*” es imposible listar todos los elementos de un conjunto infinito. No vale poner puntos suspensivos y quedarse tan pancho. Necesitaremos un nuevo axioma para poder hablar del conjunto de los números naturales.

Daremos un conjunto por **comprensión** cuando tengamos una propiedad referente a los elementos de un conjunto ya dado X y nos quedemos con el conjunto de los elementos de X que tienen esa propiedad. Por ejemplo, suponer que hemos podido construir el conjunto \mathbb{N} de los números naturales y que sabemos que significa que un número natural es par. Entonces podemos dar por comprensión el conjunto P de los números naturales pares. Indicaremos esto de la siguiente forma:

$$P = \{x \in \mathbb{N}; x \text{ es par} \}.$$

El conjunto de las partes de un conjunto.

Si $A \subseteq S$ diremos que A es un subconjunto de S , de esta manera hemos indicado una propiedad:

Ser subconjunto.

La propiedad de ser subconjunto no está (en principio) referida a los elementos de un conjunto, la axiomática de conjuntos incluye un axioma que permite, dado un conjunto S , construir el conjunto de los subconjuntos de S . Este conjunto es llamado conjunto de las partes (o subconjuntos) de S y lo indicamos:

$$\mathcal{P}(S) = \{A; A \subseteq S\}.$$

Notemos que $\mathcal{P}(S)$ no está definido por comprensión ya que los elementos A en $\mathcal{P}(S)$ no son elementos de un conjunto ya definido. Esto es, para que pudiésemos dar $\mathcal{P}(S)$ por comprensión necesitaríamos un conjunto ?? (que no tenemos) de manera que

$$\mathcal{P}(S) = \{A \in ??; A \subseteq S\}.$$

Necesitamos un axioma que nos permita hablar del conjunto de las partes de un conjunto S .

Como consecuencia del Teorema 1.1.3 tenemos que:

$$\forall S, \emptyset \in \mathcal{P}(S),$$

por tanto $\mathcal{P}(S) \neq \emptyset$ ya que por lo menos tiene un elemento. Por otro lado siempre $S \subseteq S$ y por tanto también tenemos:

$$\forall S, S \in \mathcal{P}(S),$$

Así, podemos concluir que:

- $\forall S, \mathcal{P}(S) \neq \emptyset$ y
- si $S \neq \emptyset$ entonces $\mathcal{P}(S)$ tiene al menos dos elementos \emptyset y S .

Operaciones con conjuntos.

Aunque la axiomática de conjuntos permite definir uniones e intersecciones de conjuntos cualesquiera, vamos a restringir (en un principio) estas construcciones a los subconjuntos de un conjunto dado.

Así A y B son subconjuntos de S , el subconjunto de S de elementos a tales que $a \in A$ y $a \in B$ es llamado la *intersección* de A y B . Lo denotamos por $A \cap B$. Este conjunto puede definirse por comprensión de la siguiente forma:

$$A \cap B = \{a \in S \mid a \in A \wedge a \in B\}.$$

Notar que hemos usado \mid en lugar de $;$ en la definición anterior, esta notación también es usual.

Si $A \cap B = \emptyset$, entonces A y B se dicen *disjuntos*.

La unión $A \cup B$ de A y B es el subconjunto de elementos a tales que $a \in A$ o $a \in B$:

$$A \cup B = \{a \in S \mid a \in A \vee a \in B\}.$$

Una importante propiedad que relaciona estas operaciones entre subconjunto de $\mathcal{P}(S)$ es la siguiente.

Proposición 1.1.5 (Propiedad distributiva). *Para cualesquiera subconjuntos $A, B, C \subseteq S$,*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

DEMOSTRACIÓN. Probamos la primera y dejamos la segunda como ejercicio. Sea $a \in A \cap (B \cup C)$. Como $a \in B \cup C$, será $a \in B \vee a \in C$, y como $a \in A$ bien $a \in A \cap B \vee a \in A \cap C$. Se deduce que $a \in (A \cap B) \cup (A \cap C)$. Ahora, sea $a \in (A \cap B) \cup (A \cap C)$. Será $a \in (A \cap B) \vee a \in (A \cap C)$. En cualquier caso $a \in A \wedge a \in B \vee a \in C$. Entonces $a \in A \wedge a \in B \cup C$, o sea que $a \in A \cap (B \cup C)$. \square

Intersecciones y uniones pueden ser definidas para un conjunto arbitrario de subconjuntos de un conjunto S . Sea $\Gamma \subseteq \mathcal{P}(S)$ un tal conjunto de subconjuntos. Entonces definimos su intersección

$$\bigcap_{A \in \Gamma} A = \{a \in S \mid a \in A \ \forall A \in \Gamma\}$$

y su unión

$$\bigcup_{A \in \Gamma} A = \{a \in S \mid \exists A \in \Gamma \mid a \in A\}.$$

Si Γ es finito, digamos $\Gamma = \{A_1, A_2, \dots, A_n\}$, entonces escribimos también $\bigcap_{i=1}^n A_i$ o $A_1 \cap A_2 \cap \dots \cap A_n$ para su intersección y, análogamente, $\bigcup_{i=1}^n A_i$ o $A_1 \cup A_2 \cup \dots \cup A_n$ para su unión. Es fácil ver que las propiedades distributivas son válidas para intersecciones y uniones arbitrarias de subconjuntos: $B \cap \bigcup_{A \in \Gamma} A = \bigcup_{A \in \Gamma} (B \cap A)$, $B \cup \bigcap_{A \in \Gamma} A = \bigcap_{A \in \Gamma} (B \cup A)$.

Si $A \subseteq S$ es cualquier subconjunto, se define su *complementario* como

$$c(A) = \{a \in S \mid a \notin A\}.$$

(otras notaciones usuales para este son \bar{A} , $S - A$).

Algunas propiedades elementales son:

1. $c(\emptyset) = S$,
2. $c(S) = \emptyset$,
3. $A \cap c(A) = \emptyset$,
4. $A \cup c(A) = S$,
5. $c(c(A)) = A$.

Algo menos evidentes son las siguientes:

Proposición 1.1.6 (Morgan).

$$c\left(\bigcap_{A \in \Gamma} A\right) = \bigcup_{A \in \Gamma} c(A), \quad (1.1)$$

$$c\left(\bigcup_{A \in \Gamma} A\right) = \bigcap_{A \in \Gamma} c(A). \quad (1.2)$$

Demostración. Probamos la primera. Sea $a \in c(\bigcap_{A \in \Gamma} A)$. Entonces $a \notin \bigcap_{A \in \Gamma} A$ y, por tanto, $\exists A \in \Gamma \mid a \notin A$ o, lo que es lo mismo, $\exists A \in \Gamma \mid a \in c(A)$. Por tanto, $a \in \bigcup_{A \in \Gamma} c(A)$. Supongamos ahora $a \in \bigcup_{A \in \Gamma} c(A)$. Entonces $\exists A \in \Gamma \mid a \in c(A)$ o, lo que es lo mismo, $\exists A \in \Gamma \mid a \notin A$. Pero entonces $a \notin \bigcap_{A \in \Gamma} A$ y, por tanto, $a \in c(\bigcap_{A \in \Gamma} A)$. ■

También se cumple:

Proposición 1.1.7. Para cualesquiera dos subconjuntos $A, B \in \mathcal{P}(S)$,

$$A \subseteq B \Leftrightarrow c(B) \subseteq c(A).$$

Demostración. Si $A \subseteq B$, y $a \notin B$, entonces $a \notin A$, luego $c(B) \subseteq c(A)$. Y recíprocamente, si $c(B) \subseteq c(A)$, entonces $A = cc(A) \subseteq cc(B) = B$. ■

Para subconjuntos $A, B \in \mathcal{P}(X)$, es usual también construir el subconjunto

$$A \setminus B = \{a \in A \mid a \notin B\} = A \cap c(B).$$

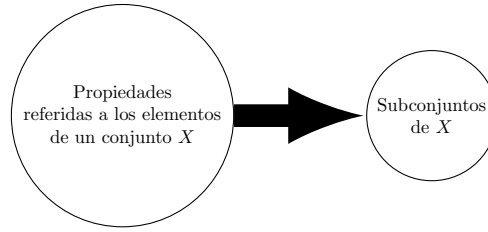
1.1.1 Proposiciones y Demostraciones.

Hemos aceptado que si tenemos una propiedad P referida a los elementos de un conjunto X podemos dar, por comprensión, el subconjunto de los elementos de X que tienen la propiedad P :

$$X_P = \{a \in X \mid a \text{ satisface } P\}.$$

Por ejemplo, si \mathbb{Z} es el conjunto de los números enteros, entonces $\mathbb{N} = \{x \in \mathbb{Z} \mid x \geq 0\}$ es el conjunto de los números naturales, o enteros no negativos.

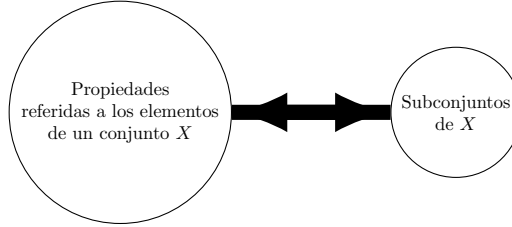
De esta manera podemos asociar a cada propiedad referida a los elementos de un conjunto X un elemento de $\mathcal{P}(X)$:



También podemos ir en sentido contrario. Esto es, a cada subconjunto $A \subseteq X$ le podemos asociar la propiedad referida a los elementos de X :

$$P_A = \text{“ser elemento de } A\text{”}.$$

De manera que tenemos una equivalencia entre las propiedades referidas a los elementos de X y los subconjuntos de X .



Esta equivalencia nos permite trasladar conceptos de un contexto a otro. De manera que los operadores lógicos corresponden a operaciones en conjuntos. Así por ejemplo:

Si P y Q son propiedades referidas a los elementos de un conjunto X , la propiedad $P \wedge Q$, leída como “ P y Q ”, es aquella que es satisfecha exactamente por los elementos que satisfacen tanto P como Q . De manera que:

$$X_{P \wedge Q} = \{x \in X \mid x \in X_P \wedge x \in X_Q\} = X_P \cap X_Q.$$

Decimos entonces que el conectivo lógico \wedge equivale a la operación \cap .

Análogamente, la propiedad $P \vee Q$, leída como “ P o Q ”, se define como aquella que satisfacen exactamente los que satisfacen P o satisfacen Q . De forma que

$$X_{P \vee Q} = \{x \in X \mid x \in X_P \vee x \in X_Q\} = X_P \cup X_Q.$$

La propiedad que es verificada por aquellos elementos sobre los que una propiedad P es falsa, es denotada por $\neg P$, y leída como “no P ”. Así que

$$X_{\neg P} = \{x \in X \mid x \notin X_P\} = c(X_P).$$

Operador lógico		Operación en conjuntos	
y	\wedge	\cap	intersección
o	\vee	\cup	unión
no	\neg	c	complementario

Table 1.1: Correspondencia operador lógico vs operación conjuntista

Podemos sintetizar esto en la siguiente Tabla 1.1.1:

Una *proposición matemática* es una relación entre dos propiedades P , Q referidas a los elementos de un conjunto X , del tipo $P \Rightarrow Q$, que leemos “ P implica Q ”, y significa que si un elemento de X satisface la propiedad P entonces ese elemento también satisface la propiedad Q .

Esto es:

La proposición $P \Rightarrow Q$ será verdad si $X_P \subseteq X_Q$.

Demostrar una proposición $P \Rightarrow Q$ consistirá precisamente en probar la inclusión $X_P \subseteq X_Q$.

La negación de este hecho que escribimos $P \nRightarrow Q$, significa entonces que $X_P \not\subseteq X_Q$, esto es que:

$$\exists a \in X_P; a \notin X_Q.$$

Así:

La falsedad de una proposición, se demuestra con un *contraejemplo*.

Una propiedad fundamental en el manejo de las proposiciones es la siguiente

Proposición 1.1.8 (Transitividad). *Sean P , Q y R propiedades referidas a los elementos de un conjunto X . Si $P \Rightarrow Q$ y $Q \Rightarrow R$, entonces $P \Rightarrow R$.*

Demostración. Si $X_P \subseteq X_Q \subseteq X_R$, entonces $X_P \subseteq X_R$. ■

Cuando se satisface $P \Rightarrow Q$ y $Q \Rightarrow P$, decimos que las propiedades P y Q son *equivalentes*. Será por que $X_P = X_Q$.

Expresamos este hecho simbólicamente por $P \Leftrightarrow Q$, leído como:

Un elemento satisface P si y solo si satisface Q , o P se satisface cuando y solo cuando Q lo hace.

El siguiente hecho es un recurso muy utilizado en demostraciones.

Proposición 1.1.9. *Sean P_1, \dots, P_n , una lista de propiedades referidas a los elementos de un conjunto X . Si se satisface que $P_1 \Rightarrow P_2, P_2 \Rightarrow P_3, \dots, P_{n-1} \Rightarrow P_n$ y $P_n \Rightarrow P_1$, entonces $P_i \Leftrightarrow P_j$ para todo i, j .*

Demostración. Es consecuencia de la transitividad: Si $i < j$, tenemos que $P_i \Rightarrow P_j$ y también $P_j \Rightarrow P_1 \Rightarrow P_i$. ■

Proposición 1.1.10. *Para cualesquiera dos subconjuntos $A, B \in \mathcal{P}(X)$,*

$$A \subseteq B \Leftrightarrow c(B) \subseteq c(A).$$

Demostración. Si $A \subseteq B$, y $a \notin B$, entonces $a \notin A$, luego $c(B) \subseteq c(A)$. Y recíprocamente, si $c(B) \subseteq c(A)$, entonces $A = cc(A) \subseteq cc(B) = B$. ■

El siguiente hecho también es un recurso muy utilizado en demostraciones.

Proposición 1.1.11. Sean P y Q propiedades referidas a elementos de un conjunto X . Las siguientes proposiciones son equivalentes (en el sentido de que se satisface una si y solo si se satisface la otra, por tanto demostrar una es equivalente a demostrar la otra):

- (i) $P \Rightarrow Q$.
- (ii) $\neg Q \Rightarrow \neg P$.

Demostración. $X_P \subseteq X_Q$ equivale a que $c(X_Q) \subseteq c(X_P)$. ■

Cuando uno demuestra $\neg Q \Rightarrow \neg P$ para probar $P \Rightarrow Q$, se dice que razonamos el **contrareciproco** de la proposición original.

También se suele decir que demostramos $P \Rightarrow Q$ *por reducción al absurdo*: Supongamos que un elemento verifica P pero no Q . Entonces verifica $\neg Q$ y, por tanto, $\neg P$. Es decir, que no verifica P en contradicción a la hipótesis.

EJERCICIOS

En los siguientes enunciados, A, B, C, \dots refieren a subconjuntos arbitrarios de un conjunto dado X , y se pide demostrar la veracidad de las equivalencias o igualdades propuestas.

1. $A \subseteq B \Leftrightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$.
2. $A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$.
3. (a) $A \cap B = \emptyset \Leftrightarrow A \subseteq c(B) \Leftrightarrow B \subseteq c(A)$.
(b) $A \cup B = X \Leftrightarrow c(A) \subseteq B \Leftrightarrow c(B) \subseteq A$.
4. $(A - B) \cap (A - C) = A - (B \cup C)$.
5. (a) $A - B = A \Leftrightarrow A \cap B = \emptyset$.
(b) $A \cap (B - C) = (A \cap B) - (A \cap C)$.
6. Siendo la "diferencia simétrica" $A \Delta B$ de A y B el subconjunto

$$A \Delta B = (A - B) \cup (B - A),$$

- (a) $A \Delta B = (A \cup B) - (A \cap B)$.
- (b) $A \Delta B = B \Delta C$.
- (c) $A \Delta \emptyset = A$.
- (d) $(A \Delta B) \Delta C = A \Delta (B \Delta C)$
- (e) $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$.

7. Si A y B son finitos, $|A \cup B| + |A \cap B| = |A| + |B|$.

8. Si A , B , y C son finitos,

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

En los siguientes enunciados, P, Q, R, \dots refieren a propiedades que pueden ser satisfechas, o no, por los elementos de un conjunto X . Se pide demostrar la veracidad de las proposiciones o propuestas siguientes.

9. (a) $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$.
 (b) $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$.

10. Las siguientes proposiciones son equivalentes:

- (a) $P \Rightarrow Q$.
 (b) $P \vee Q \Leftrightarrow Q$.
 (c) $P \wedge Q \Leftrightarrow P$.

11. (a) $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$.
 (b) $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$.

12. $(P \vee \neg Q) \vee (P \vee \neg R) \Leftrightarrow P \vee \neg(Q \wedge R)$.

13. $P \vee Q \vee \neg Q \Leftrightarrow P \vee Q \vee \neg(P \vee R)$.

14. $(P \vee \neg Q) \wedge (Q \vee \neg P) \Leftrightarrow (P \wedge Q) \vee \neg(P \vee Q)$.