Apuntes Sobre Algebra

Nota preeliminar

Este apunte como bien lo dice su nombre es simplemente un apunte. En muchos casos los conceptos se presentan sin demostracion alguna o con demostraciones y definiciones simplificadas. Para mayor rigor en las demostraciones y definiciones revisar la bibiografia especificada al final es lo adecuado.

Logica

Antes de empezar es importante definir cieros simpolos que seran utilizados para hablar de logica.

$\forall$ x Para todo x
$\exists$ x Existe algun x
$\rightarrow$ implicancia, entonces
$\leftrightarrow$ Si y solo si (sii)
-P negacion, no P
$\wedge$ conjuncion , y
$\vee$ disyuncion, o

Tambien simplificaremos a verdadero como V y a falso como F.

Ahora veamos un poco más especificamente que significan los símbolos anteriomente mencionados. Para hacer esto introduciremos un nuevo concepto, simple pero muy útil. La tabla de verdad. La manera mas facil de entenderls es mirarla. Aqui va una.

P	**Q**	**-P**	**P $\wedge$ Q**	**P $\vee$ Q**
V	*V*	F	V	V
V	*F*	F	F	V
F	*V*	V	F	V
F	*F*	V	F	F

La tabla define la negacion, conjuncion y disyuncion. Como se ve la tabla propone dos eventos. P y Q y analiza la verasidad o no de distintas popocisiones dadas todas las posibles compinaciones de P y Q. Notese que la conjuncion y disyuncion son conmutativas. Estas tambien son asociativas, pero dejamos esta tabla de verdad para el lector.

Aqui la tabla de verdad de $\rightarrow$ *y* $\leftrightarrow$ (entonces y si y solo si)

P	**Q**	**P $\rightarrow$ Q**	**P $\leftrightarrow$ Q**
V	*V*	V	V
V	*F*	F	F
F	*V*	V	F
F	*F*	V	V

Llamaremos a estos simpolos que acabamos de definir como conectivos logicos. Los dos no definidos ($\forall, \exists$) seran llamados cuantificadores (para todo y existe algun). Notese que estos dos no implican mas de lo que dicen. Ya aprenderemos a usarlos. correctamente pero antes veamos que pasa si combinamos algunos de los conectivos logicos que aprendimos.

Antes de seguir una aclaracion sobre la implicancia. Decimos que Q es necesaria para P. Y que P es suficiente para Q.

Veamos un ejemplo. Es madre entonces es mujer. Madre = P Mujer = Q

Es necesario se mujer para poder ser madre

Es suficiente ser madre para ser mujer. (No tome en cuenta cuestiones de infertilidad o falta de hombres).

Tambien puede verse con una tabla de valores que $P \to Q = -P \vee Q$

Las leyes de morgan

$$-(P \wedge Q) = -P \vee -Q$$

$$-(P \vee Q) = -P \vee -Q$$

Estas equivalencias pueden ser comprobadas rapidamente con un tabla de verdad.

Como dijimos la implicancia puede ser expresada como $-P \vee Q$ con lo que la negación de la esta será

$$-(P \to Q) = P \wedge -Q$$

Tambien vale la pena aclarar las negaciones de los cuantificadores.

$$-\forall = \exists$$

$$-\exists = \forall$$

Otras cosas.
Tautologias. Son expresiones logicas las cuales simpre son verdaderas.
Contradiciones. Expreciones logicas simpre falsas.

Implicaciones Logicas
La mayoria de estas tienen nombres extranos o no tan, lector, si esto lo confunde no preste atencion (a los nombres unicamente).
Notese tambien que se utilizara un nuevo simbolo ($\Rightarrow$). Este quiere decir: implica o se concluye.

Modus Ponens: $p \wedge (p \to q) \Rightarrow q$

Modus Tollens: $-q \wedge (p \to q) \Rightarrow -p$

Silogismo Disyuntivo: $(p \wedge q) \wedge -q \Rightarrow p$

Simplificacion: $p \wedge q \Rightarrow p$

Adicion: $p \Rightarrow p \vee q$

Silogismo Hipotetico: $(p \to q) \wedge (q \to r) \Rightarrow p \to r$

Uno mas: $(p \wedge q) \to r \Leftrightarrow p \to (q \to r)$

Leyes distributivas

$$(p \wedge q) \vee r \Leftrightarrow (p \vee r) \wedge (q \vee r)$$

$$(p \vee q) \wedge r \Leftrightarrow (p \wedge r) \vee (q \wedge r)$$

Los Naturales

Factorial, Conbinaciones y Permutaciones.

Definiciones:

Factorial
$N! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot \ldots \cdot N$ se lee N factorial
$0! = 1$

Combinaciones.
$C(p,n) = \binom{p}{n} = \frac{p!}{n!(p-r)!}$ se lee Combinaciones de p tomados de a n

Permutaciones

$P(p,n) = \frac{p!}{(p-r)!}$ se lee Permutaciones de p tomados de a n

Sumatoria y Productoria.

Esta seccion se trata unicamente de notacion.

Entendemos por una sumatoria a lo siguiente:

$$\sum_{i=}^{n} x_i = x_1 + x_2 + x_3 + x_4 + \ldots + x_n$$

Y por productoria entendemos lo siguiente.

$$\prod_{i=1}^{n} x_i = x_1 \cdot x_2 \cdot x_3 \cdot x_4 \cdot \ldots \cdot x_n$$

No hay mucho mas que entender. Se puede realizar conjeturas sobre que pasa y como operar con productorias y sumatorias mas complejas, pero todas se deducen de las definiciones anteriomente mencionadas.

Binomio de Newton

Definicion:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

No hay mucho mas que decir. Sientese un rato mire como funciona la formula y si no le cree lea la siguiente seccion y una vez aprendidos los principios de inducion pruebe que el binomio es correcto.

Induccion

Basicamente el principio de induccion dice lo siguiente. Si una propocicion es verdadera para un primer elemento de un conjunto, y suponiendo valida la poposicion para un cierto elemento n , si puede ser probado que n + 1 es verdadero entonces sera verdadero para cualquier elemento del conjunto. Vale acara que el unico conjunto de numero para que funcionan los principios de inuccion completa es el de los numeros naturales.

Repetimos.
Probamos validez para primer elemento P(1)
Suponemos valido para un elemento P(n). Llamamos a esto Hipotesis Inductiva.
Probaremos ahora, usando la hipotesis, que vale para un elemento P(n+1). A esto lo llamamos tesis.
Si vale para P(1) y suponiendo la hipotesis como verdadera se puede probar que P(n+1) es verdadera, entonces la premisa es valida para cualquier n mayor o igual a 1.

Numeros Enteros (Z)

Divisibilidad

Notacion:
A|B se lee A divide a B

Definicion:
$A \mid B \leftrightarrow ax = b, x \in Z$

Sean a,b,c enteros se demostraran varias propiedades.
(no se alarara en cada caso que la los enteros son cerrados en el producto y la suma)

1. - $a \mid 0, \forall a \in Z$
$ax = 0, x \in Z, a \cdot 0 = 0, como\ 0 \in Z\ vale\ la\ afirmacion$

2.- $a \mid b \wedge b \mid c \rightarrow a \mid c$
$ax = b, x \in Z \wedge by = c, y \in Z \rightarrow (ax)y = axy = c \rightarrow a \mid c$

3.- $a \mid b \rightarrow a \mid -b \wedge -a \mid b$
$ax = b, x \in Z \rightarrow (-1)ax = (-1)b \rightarrow a(-x) = -b \rightarrow a \mid -b$
$ax = b, x \in Z \rightarrow (-1)(-1)ax = b \rightarrow -a(-x) = b \rightarrow -a \mid b$

4.- $a \mid b \wedge a \mid c \rightarrow a \mid (b+c) \wedge a \mid (b-c)$
$ax = b, x \in Z \wedge ay = c, x \in Z \rightarrow ax + ay = a(x+y) = b + c \rightarrow a \mid (b+c)$
$ax = b, x \in Z \wedge ay = c, x \in Z \rightarrow ax - ay = a(x-y) = b - c \rightarrow a \mid (b-c)$

Dejamos las siguientes como ejercicio para el lector.

1. $a \mid b \rightarrow a \mid bc$
2. $a \mid (c+b) \wedge a \mid b \rightarrow a \mid c$
3. $0 \mid a \rightarrow a = 0$
4. $a(a+1) = 2b$
5. $a \mid b \wedge b \mid a \leftrightarrow a = b$

Las siguientes son falsas. Demostrar esto proponiendo un ejemplo donde no se cumplen.

1. $a \mid b.c \rightarrow a \mid b \vee a \mid c$
2. $a \mid (c+b) \rightarrow a \mid b \vee a \mid c$
3. $a \mid b \wedge c \mid b \rightarrow a.c \mid b$

Algoritmo de la division

Notacion y defincion

A= B(q)+ r Al dividir a por b se tiene un cociente (q) y un resto (r).
Nota: r debe ser positivo

Primos
Se dice que un numero X es primo si admite exactamente 4 divisores (1, -1, X, -X).

Maximo Comun Divisor (MCD)

Notacion
(A,B)= R se lee el maximo comun divisor de A y B es R

Definicion:
1. $R > 0$
2. $R|A$ y $R|B$
3. Si $x|A$ y $x|B$ entonces $x|R$

Propiedad:
R=Am +Bn con m y n pertenecientes a Z

Coprimos:
Se dice que A y B son coprimos si y solo si (A,B)=1

Teorema de Euclides sobre el MCD

Por el algoridmo de la division:
A=qB + r
Se tiene que por el teorema de euclides:
(A,B)=(B,r)

Entonces si se quiere hayar el MCD se aplica el teorema de esta manera:
$A=Q_1\ B+R_1$
$B=R_1\ Q_2+R_2$
$R_1=R_2\ Q_3+R_3$
$R_2=R_3\ Q_4+R_4$

$(A,B)=(B,R_1)=(R_1,R_2)= (R_2,R_3)= (R_3,R_4)$

Se sigue asi hasta que $R_x = 0$. En ese entonces R_{x-1}=MCD

Minimo Comun Multiplo

Notacion:
[a,b] se lee el minimo comun multiplo de a y b

Definicion:
$$[a,b] = \frac{|a.b|}{(a,b)}$$

Ejercicios de parcial:
Resolver los siguientes utilizando los conceptos de MCD, divisibilidad, MCM y el teorema de Euclides.
En todos los casos a,b,c pertenecen a Z

1. Encontrar a y b tales que (a,b)=84 y [a,b]=810
2. Demostrar $(a,b) = 1 \rightarrow (a, a+b) = 1$
3. Demostrar $(a,b) = 1 \rightarrow (a, b \cdot c) = (a,c)$
4. Demostra si a y b no son simultaniamente nulos $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)} \right) = 1$

Teorema fundamental de la Aritmetica (TFA)

Definicion:

Cualquier numero pertieneciente a Z distinto a 1, -1, 0 puede ser escrito como un poducto finito de primos con su correspondiente signo. Este producto es unico salvo su orden.

Mas tecnicamente:

Si $n \in Z$

$$n = \varepsilon \cdot \prod_{i=1}^{k} p_i = \varepsilon \cdot p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot \ldots \cdot p_k$$

donde $\varepsilon = -1 \vee \varepsilon = 1$ y p_i es un numero primo.

Teoria de Conjuntos

En principio no se definira un conjuntos sino las operiaciones que se pueden realizar con ellos. La naturaleza de un conjunto se entendera al tabajar con ellos.

Pertenencia:

$x \in A$ se lee x pertenece a A donde x es un elemento y A es un conjunto.

Se dice que $x \in a$ sii x es un elemento que conforma a A.

Notese que los elementon se caracterizaran con letras minusculas mientras que los conjuntos con mayusculas.

Asimismo la no pertenencia

$x \notin A$ se lee x no pertenece a A

Esto quiere decir que x no forma parte de los elementos de A.

Definiendo Conjuntos

Un conjunto, en principio puede ser definido de dos maneras: por extension y por compresion.

Aqui ejemplos:

Por compresion:

Q={x: x es un gato} Q seria el conjunto de los gatos.

M={p: p $\in$ Z) M es el conjunto de los numero enteros.

K={j: $7 < j < 22 \wedge j \in Z$ } K es el conjunto de numeros enteros ente 7 y 22.

Por extension:

H={Agustina, Eleonora, Paula}H es el conjunto de mis hermanastras.

P={123, Rigoberto, $\sqrt{\Omega}$ } P es el conjunto con esos tres elementos.

Inclusion o Contencion

Notacion:

$F \subset G$ Se lee F esta incluido en G

F esta contenido en G

G contiene a F , etc.

Definicion

Antes de dar la definicion formal es importante aclarar que cuando se definia pertenencia se estaba hablando de elementos que pertenecian a conjuntos. La inclusion se refiere a conjuntos que estan *contenidos* en otros conjuntos, o que son subconjuntos de estos.

Pertenencia : elemento $\in$ conjunto

Inclucion: conjunto $\subset$ conjunto

Ahora si, un conjunto A esta contenido otro B sii todos los que pertenescan a A tambien pertenecen a B.

$$A \subset B \leftrightarrow (x \in A \rightarrow x \in B)$$

La no contencion.

Para dar una formula general para la no contencion basta con negar la contencion y aplicando las leyes de morgan se llega a que:

$$A \not\subset B \leftrightarrow (x \in A \wedge x \notin B)$$

Igualdad

Se dice que dos conjuntos son iguales sii cada uno esta incluido en el otro.

$$A = B \leftrightarrow A \subset B \wedge B \subset A$$

El conjunto Vacio

El conjunto vacio es aquel que no tiene ningun elemento dentro de el y se lo define y anota de la siguiente manera.

$\varnothing = \{x: x \neq x\}$

Universo

Definir el concepto de universo es complicado y puede llevar a contradicciones. Si embargo cuando se hable de universo nos refiriremos a un conjunto que incluya a todos los conjuntos que se trabaja, y si se desea un poco mas. Al universo lo denotaremos como: U.

Partes de un conjunto

Notacion:
P(W) se lee: el conjunto de las partes de W.

Definicion:
Dado un conjunto A se llama P(A) al conjunto cuyos elementos son todos los subconjuntos de A.

$$\mathrm{P(A)} = \{\mathrm{B}:\mathrm{B} \subset A)$$
$$\mathrm{x} \in \mathrm{P(A)} \leftrightarrow \mathrm{x} \subset A$$

Si un conjuntoA tiene n elementos entonces el conjunto de P(A) tendra 2^n elementos.

Opreraciones entre Conjuntos

En cada caso se presenta la regla general en letra grande y a continuacion propiedades que pueden ser demostradas por el lectos simplemente aplicando las definiciones.

Union

$$x \in (A \cup B) \leftrightarrow x \in A \vee x \in B$$

Propiedades:
Es asociativa y conmutativa.
$A \cup \varnothing$ =A
$A \cup A = A$
P(A) $\cup$ P(B) $\subset$ P(A $\cup$ B)

Interseccion

$$x \in (A \cap B) \leftrightarrow x \in A \wedge x \in B$$

Propiedades:
Es asociativa y conmutativa.
A $\cap \varnothing = \varnothing$
A $\cap$ A=A
P(A) $\cap$ P(B)=P(A $\cap$ B)

Leyes distibutivas de la intersecion y la union
$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$
$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$

Diferencia

$$x \in (A - B) \leftrightarrow x \in A \wedge X \notin B$$

Propiedades:
No es conmutativa ni asociativa.
(A-B)-C $\subset$ A-(B-C)
A-A = $\varnothing$
A-$\varnothing$ = A
$\varnothing$-E = $\varnothing$
Si A-B = B-A $\rightarrow$ A=B=$\varnothing$

Utilizando estras tres operaciones se puede demostrar que:
A-(B-C) = (A-B) $\cup$ (A $\cap$ C)
A $\cup$ (B-C) = (A $\cup$ B)-(C-A)
A $\cap$ (B-C) = (A $\cap$ B)-(A $\cap$ C)

Diferencia Simetrica

$$x \in (A \Delta B) \leftrightarrow x \in (A \cup B) \wedge x \notin (A \cap B)$$

Propiedades:
Es conmutativa y asociativa

$A \Delta \varnothing = A$
$A \Delta A = \varnothing$
Distributiva con respecto a la intersecion.
$(A \Delta B) \cap C = (A \cap C) \Delta (A \cap C)$

Complemento

$$x \in A^c \leftrightarrow x \notin A \wedge x \in U$$

Morgan otra vez:
$(A \cap B)^c = A^c \cup B^c$
$(A \cup B)^c = A^c \cap B^c$

Par Ordenado y Producto Cartesiano
El par ordenado (a, b) es un conjunto cuyos elementos son {a} y {a,b}

$$(a,b) = \{\{a\},\{a,b\}\}$$

Producto carteciano entre A y B es el conjunto de todos los pares ordenados cuyas primeras componentes pertenecen a A y segundas a B.

$$(x,y) \in (A \times B) \leftrightarrow x \in A \wedge y \in B$$

El producto cartesiano es distributivo con respecto a la interseccion, la union y la diferencia. No es conmutativo ni asociativo.

Graficas
Se denomina a un conjunto G como una grafica solo si sus elementos son pares ordenados.

Si (x,y) es un par ordenado que conforma una grafica G. Se llama primera projecion (Pr_1G)de G a x, y segunda (Pr_2G) a y.

$$x \in \mathrm{Pr}_1\, G \leftrightarrow (x,y) \in G$$

$$y \in \mathrm{Pr}_2\, G \leftrightarrow (x,y) \in G$$

Correspondencia o relacion
Si esta definicion parece inutil para el lector, no se preocupe mucho. Siga adelante.

Se define como correspondencia o relacion a la terna ordenada r = (G,A,B) donde G es una grafica, $Pr_1G \subset A$ y $Pr_2G \subset B$. Se dice que G es la grafica de r, A el conjunto de partida y B el conjunto de llegada de r.

Funciones

Se dice que *f* es una funcion de A en B si *f* hace coresponder a todos elementos de A en solo un elemento de B.

$$f: A \rightarrow B$$

Se dice que r = (G, A, B) es una relacion funcional si: $f: A \rightarrow B$.
Se dice que G es una grafica funcional si: $f: Pr_1G \rightarrow Pr_2G$.

Imagen
Si se tiene una reacion r = (G, X, Y) se llama imagen de x por r al conjunto de elementos que corresponden a X por r.
A la imagen de X por r se la anota como: r(X)
Entonces: $y \in f(A) \Leftrightarrow \exists x \in A \wedge f(x) = y$

Propiedades
$f(A \cup B) = f(A) \cup f(B)$
$f(A \cap B) \subset f(A) \cap f(B)$

Composicion
Composicion de G_1 en G_2:
$$(x,z) \in G_1 \circ G_2 \leftrightarrow (x,y) \in G_2 \wedge (y,z) \in G_1$$
Es asociativa pero **no** conmutativa.

Inyectividad

Se dice que una funcion *f:*A $\rightarrow$ B es inyectiva o 'uno a uno' si y solo si:
$$\forall x \forall x' \in A : f(x) = f(x') \rightarrow x = x'$$
o bien
$$\forall x \forall x' \in A : x \neq x' \rightarrow f(x) \neq f(x')$$

Sobreyectividad
Se dice que una funcion *f:*A $\rightarrow$ B es sobreyectiva o suryectiva si y solo si:
$$\forall y \in B, \exists x \in A / f(x) = y$$
Todo elemento de la imagen es la corespondencia por f de algun elemento del dominio.

Biyectividad
Se dice que f es biyectiva si y solo si es inyectiva y sobreyectiva.

Propiedades
f y g son biyectivas $\rightarrow$ $f \circ g$ es biyectiva
f y g son inyectivas $\rightarrow$ $f \circ g$ es inyectiva
f y g son sobreyectivas $\rightarrow$ $f \circ g$ es sobreyectiva
$f \circ g$ es sobreyectiva $\rightarrow$ f *es* sobreyectiva
$f \circ g$ es inyectiva $\rightarrow$ g es inyectiva
$f \circ g \wedge g \circ h$ son biyectivas $\rightarrow$ *g, f, h* son biyectivas

Inversa
Se denomina inversa de G a la grafica G^{-1} tal que:
$(x,y) \in G \leftrightarrow (y,x) \in G^{-1}$

Propiedades:
$(x,y) \in (G_1 \circ G_2)^{-1} = (x,y) \in (G_2^{-1} \circ G_1^{-1})$ Notese que se alternan las graficas.

Relaciones

Veremos especificamente relaciones binarias, es decir, relaciones en las que se vinculan dos elementos de dos conjuntos ya sean estos ultimos diferentes o iguales.

Sea R una relacion y A,B dos conjuntos.
Se dira que R es una relacion entre A y B $\leftrightarrow R \subset A \times B$
Se dira que un par ordenado (a,b) esta relacionado si pertenece a R
$(a,b) \in R$ o bien aRb

Propiedades de las relaciones
En general podemos clasificar una relacion $R \subset A^2$ con las cuatro propiedades que siguien:

Reflexividad
Donde:
R es reflexiva $\leftrightarrow \forall x : x \in A \rightarrow (x,x) \in R$
R es no reflexiva $\leftrightarrow \exists x \in A \wedge (x,x) \notin R$
R es areflexiva $\leftrightarrow \forall x : x \in A \rightarrow (x,x) \notin R$

Simetria
R es simetrica $\leftrightarrow \forall x, \forall y \in A,\ (x,y) \in R \rightarrow (y,x) \in R$
R es no simetrica $\leftrightarrow \exists x, \exists y \in A,\ (x,y) \in R \wedge (y,x) \notin R$
R es asimetrica $\leftrightarrow \forall x, \forall y \in A,\ (x,y) \in R \rightarrow (y,x) \notin R$

Transitividad
R es transitiva $\leftrightarrow \forall x, \forall y, \forall z : (x,y) \in R \wedge (y,z) \in R \rightarrow (x,z) \in R$
R es no transitiva $\leftrightarrow \exists x, \exists y, \exists z : (x,y) \in R \wedge (y,z) \in R \wedge (x,z) \notin R$
R es atransitiva $\leftrightarrow \forall x, \forall y, \forall z : (x,y) \in R \wedge (y,z) \in R \rightarrow (x,z) \notin R$

Antisimetria
R es antisimetrica $\leftrightarrow \forall x, \forall y,\ (x,y) \in R \wedge (y,x) \in R \rightarrow x = y$

Relaciones de Equivalencia

Notacion
Sea R un relacion $R \subset A^2$

Si un par (a,b) pertenece a la relacion de equivalencia se anotara a ~ b.

Definicion
R es de equivalencia si y solo si
R es reflexiva, simetrica y transitiva.

Bibliografia

Notas de Algebra, Enzo Gentile, Ediciones Colihue EUDEBA
Introduccion a la teoria de Conjuntos, Lia Oubiña, EUDEBA
Algebra I, Armando o. Rojo, El Ateneo