Recordar revisar las notas (N1)

Definición 1. Un ***grupo*** es una terna ordenada $(G, *, e)$ que consta de un conjunto no vacío G, una operación $*\colon G \times G \to G$ y un elemento distinguido $e \in G$ que satisfacen las siguientes propiedades

(A) Asociatividad: Para cualesquiera $a, b, c \in G$, $a * (b * c) = (a * b) * c$.

(N) Neutro: Para cualquier $g \in G$, $g * e = e * g = g$.

(I) Existencia de inversos: Para cada $g \in G$, existe $g' \in G$ tal que $g * g' = g' * g = e$.

Si además la operación $*$ satisface

(C) Conmutatividad: Para cualesquiera $a, b \in G$, $a * b = b * a$.

decimos que el grupo es ***abeliano*** o *conmutativo*.

La operación de un grupo abeliano suele denotarse mediante el símbolo $+$ cuando se entiende que "es como" una suma usual, en lugar de $*$; o bien, mediante $\cdot$ cuando se comporta como un producto. Más adelante este tipo de convención se irá aclarando.

Ejemplo: Si X es un cto, ent. la colección de funciones biyectivas de X en X, denotada

$$S_X = \{ f : X \to X \mid f \text{ es biyectiva} \},$$

es un grupo con la sigte. operación

$$* : S_X \times S_X \to S_X$$
$$(f, g) \longmapsto f \circ g$$

Neutro: La función $Id : x \in X \mapsto x \in X$ es biyectiva. Más aún

$\forall f$ función biyectiva, $f \circ Id = Id \circ f$.

En efecto:

Si $p \in X$, ent. $f \circ Id(p) = f(Id(p))$
$= f(p)$

$$Id \circ f(p) = Id(f(p)) = f(p).$$

Como $p \in X$ fue arbitrario, $f \circ Id = Id \circ f$.

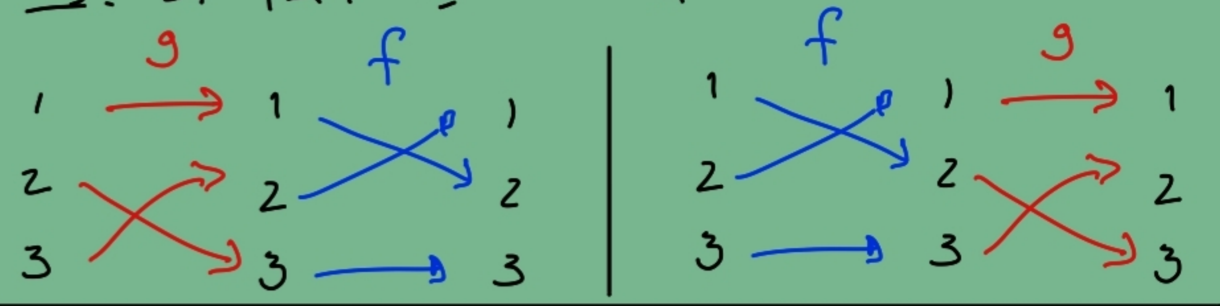
Inversos: Dada $f \in S_X$, por ser f biyectiva se tiene

$\exists\, f^{-1}$ biyectiva tq $f \circ f^{-1} = f^{-1} \circ f = Id.$

Asociatividad: Por Álg. Sup I ó Cálculo I, es bien sabido que la composición de funciones es asociativa.

$\therefore\ (S_{\mathbb{X}}, \circ, Id)$ es un grupo. $\blacksquare$

Obs. Si $|\mathbb{X}| \geq 3$ ent. $S_{\mathbb{X}}$ no es conmutativo.



$\Rightarrow$ $\boxed{f \circ g(1) = 2 \quad \text{vs.} \quad g \circ f(1) = 3}$

$\therefore\ f \circ g \neq g \circ f.$

Prop. Si G es un gpo, ent. $\exists\, \mathbb{X}$ cto $\exists\, \Gamma \subseteq S_{\mathbb{X}}$ subgrupo de $S_{\mathbb{X}}$ tq $G \cong \Gamma$ donde $\cong$ significa que hay una función biyectiva

$$\varphi : G \to \Gamma \quad \text{tq} \quad \forall\, x, y \in G,\ \varphi(x *_G y) = \varphi(x) \circ \varphi(y)$$

Subgrupo $\Gamma \leq S_{\mathbb{X}}$ significa que $\circ|_{\Gamma} : \Gamma \times \Gamma \to S_{\mathbb{X}}$ hace que $(\Gamma, \circ|_{\Gamma}, Id)$ sea gpo.

Definición 2. Un *campo* es una quinteta ordenada $(\mathbb{F}, +, \times, 0, 1)$ que consta de un conjunto $\mathbb{F}$, dos operaciones $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$, $\times : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ y elementos distinguidos $0, 1 \in \mathbb{F}$, tales que

- $0 \neq 1$. Si no lo pidiéramos, $\{0 = 1\}$ sería campo.
- $(\mathbb{F}, +, 0)$ es un grupo abeliano. $+$ se llama adición o suma
- $(\mathbb{F} \setminus \{0\}, \times, 1)$ es un grupo abeliano. En este caso, suele denotarse $\mathbb{F}^{\times} := \mathbb{F} \setminus \{0\}$. Se llama multiplicación o producto
- $\times$ se "distribuye" sobre $+$: Para cualesquiera $a, b, c \in \mathbb{F}$, $a \times (b + c) = a \times b + a \times c$.

Obs. 0 no puede pertenecer al gpo $(\mathbb{F}^{\times}, \times, 1)$ ya que, la propiedad

$$\forall p \in \mathbb{F}, \quad 0 \times p = 0$$

implica que, si hubiera 0^{-1}, ent.

$$0 = 0 \times 0^{-1} = 1 \rightsquigarrow 0 = 1 \;\;\text{\Large ⊠}$$

Ejemplos de campos: $\mathbb{Q}, \mathbb{R}$ ó $\mathbb{C}$.

Yendo un poco más allá, nos podemos encontrar con los $\mathbb{Z}_p$.

Es por estos último que hacemos un breve repaso sobre algunos hechos que ocurren en $\mathbb{Z}$ (ver Notas N1).

En lo que resta de la subsección, hablaremos un poco de los anillos $\mathbb{Z}_n$ (con $n \in \mathbb{N}$). Para un exposición mucho más detallada consulte el libro **Álgebra Superior: Curso Completo** de ***Carmen Gómez Laveaga***. Recordemos que

- $\mathbb{Z}$ es un anillo conmutativo con unidad. Esto es: tiene dos operaciones, $+, \cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, tales que
  1. $(\mathbb{Z}, +, 0)$ es grupo abeliano; y
  2. $(\mathbb{Z}, \cdot, 1)$ no es un grupo, no obstante la operación $\cdot$ es asociativa, tiene neutro y es conmutativa. Una estructura con estas propiedades es llamada *monoide conmutativo*.
- Si bien la operación $\cdot$ no tiene inversos siempre, sí nos da una noción de *divisibilidad*: Dados $a, b \in \mathbb{Z}$, diremos que ***a* divide a *b***, o que *b es divisible por a*, si existe $q \in \mathbb{Z}$ tal que $b = a \cdot q$. Si a divide a b, lo denotamos como $a \mid b$; si no lo divide, entonces usamos $a \nmid b$.
- A partir de la definición de divisibilidad, podemos notar que 1 divide a cualquier otro entero. Se puede probar, como consecuencia del *Teorema Fundamental de la Aritmética*[1], que cada entero $k \neq 0$ tiene un número finito de divisores. Es así que introducimos la siguiente:
  Definición: Si $a, b \in \mathbb{Z}$, entonces su **máximo común divisor** es
  $$(a; b) := \max\{d \in \mathbb{Z} \mid d|a \ \wedge \ d|b\}.$$
  Se puede demostrar que $(a; b)$ coincide con el número
  $$\min\left\{k \in \mathbb{N} : \exists \lambda, \mu \in \mathbb{Z} \ (k = a\lambda + b\mu)\right\}$$

[1] Este asegura que todo entero positivo es producto de número primos y dicho producto es único salvo en el orden de la multiplicación.

- Decimos que a y b son **primos relativos** si $(a; b) = 1$. Es fácil notar que si $m, p \in \mathbb{Z}$ son tales que $p \nmid m$ y p es primo, entonces $(m; p) = 1$.
- Asimismo, en $\mathbb{Z}$ tenemos el ***Algoritmo de la División***, este establece que:
  Dados $a, b \in \mathbb{Z}$, con $b \neq 0$, existen **únicos** $r, q \in \mathbb{Z}$ tales que: $\quad a = bq + r$, donde $0 \leq r < |b|$.
  Notemos que $a \mid b$ *si, y sólo si*, $r = 0$ en $a = bq + r$.
- Sea $n \neq 0$ un entero. En $\mathbb{Z}$ se puede definir la siguiente **relación de equivalencia**[2]:
  $$a \sim_n b \iff n \mid (b - a).$$
  La relación $\sim_n \subseteq \mathbb{Z} \times \mathbb{Z}$ es llamada "equivalencia *módulo n*" y se denota por
  $$a \equiv b \pmod{n} \qquad \text{(en este caso diríamos “}a\text{ es equivalente ó congruente a }b\text{ módulo }n\text{”)}.$$
  Si $a \in \mathbb{Z}$, usaremos $[a]$ ó $\overline{a}$ para referirnos a su clase de equivalencia, $[a]_n = \overline{a} := \{k \in \mathbb{Z} : k \equiv a \pmod{n}\}$.
- De la definición es evidente que para $k \in \mathbb{Z}$, $[k]_n = [0]_n$ *si, y sólo si*, $n \mid k$.

Recordar: Una relación $\sim \subseteq A \times A$ es de equivalencia si

R) Es reflexiva: $\forall a \in A$, $a \sim a$

S) Es simétrica: $\forall a, \tilde{a} \in A$, $a \sim \tilde{a} \Rightarrow \tilde{a} \sim a$

T) Es transitiva: $\forall a, b, c \in A$, $a \sim b$ y $b \sim c \Rightarrow a \sim c$.

- Al conjunto de *clases de equivalencia módulo n* se le denota por $\mathbb{Z}_n$ ó $\mathbb{Z}/n\mathbb{Z}$. Resulta que en $\mathbb{Z}_n = \{[k] : k \in \mathbb{Z}\}$ se tienen dos operaciones, $\hat{+}, \hat{\cdot} \colon \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$, definidas mediante las correspondencias

$$[a]\hat{+}[b] = [a+b] \quad \text{y} \quad [a] \hat{\cdot} [b] = [a \cdot b].$$

  Un hecho importante es que estas operaciones están bien definidas (esto significa que son funciones que no dependen de los representantes de las clases de equivalencia). Más aún, como resultado se obtiene que $(\mathbb{Z}_n, \hat{+}, [0])$ es un grupo abeliano, y $(\mathbb{Z}_n, \cdot)$ es asociativa, tiene neutro y es conmutativa.

- El siguiente teorema es importante porque nos dice bajo qué condiciones un $\mathbb{Z}_n$ tiene inversos multiplicativos.

Teorema 1. Sea $n \in \mathbb{N}$. Entonces $\mathbb{Z}_n$ es un campo ***si, y sólo si,*** n es un número **primo**.

La parte "fácil" de demostrar es la implicación de necesidad ($\Leftarrow$) y es como sigue:

Demostración. Si n es primo y $[k] \in \mathbb{Z}_n$ no es cero (*i.e.* $[k] \neq [0]$), entonces por observaciones previas $n \nmid k$ y por ello, siendo n primo, $(k; n) = 1$. Así, existen $\lambda, \mu \in \mathbb{Z}$ tales que $k\lambda + n\mu = 1$. Al tomar clases de equivalencia, obtenemos

$$[1] = [k\lambda + n\mu] = [k\lambda] + \underbrace{[n\mu]}_{[n][\mu]=[0][\mu]} = [k\lambda] + [0] = [k][\lambda].$$

Esto es exactamente la existencia del inverso multiplicativo de $[k] \in \mathbb{Z}_n \setminus \{[0]\}$. $\square$

En las notas viene un ejemplo donde a $\mathbb{Z}_2$ se le agrega una raíz ξ del polinomio $x^2 + x + 1$.

Definición 3. Sea $\mathbb{F}$ un campo. Un ***espacio vectorial sobre*** $\mathbb{F}$ es un conjunto V equipado con dos operaciones $+ \colon V \times V \to V$ y $\cdot \colon \mathbb{F} \times V \to V$ tales que

- $(V, +)$ es un grupo abeliano con elemento neutro $\mathbf{0}$.
- La operación $\cdot$ satisface, para cualesquiera $\alpha, \beta \in \mathbb{F}$, y $\mathbf{v}, \mathbf{w} \in V$
  - (A) Asociatividad: $\alpha \cdot (\beta \cdot \mathbf{v}) = (\alpha \times \beta) \cdot \mathbf{v}$.
  - (Id) Identidad: $1 \cdot \mathbf{v} = \mathbf{v}$
  - (Di) Distributividad izquierda: $(\alpha + \beta) \cdot \mathbf{v} = \alpha \cdot \mathbf{v} + \beta \cdot \mathbf{v}$.
  - (Dd) Distributividad derecha: $\alpha \cdot (\mathbf{v} + \mathbf{w}) = \alpha \cdot \mathbf{v} + \alpha \cdot \mathbf{w}$.

Los elementos $\mathbb{F}$ son llamados ***escalares*** y los de V son llamados ***vectores***.

Es de costumbre omitir el punto $\cdot$ en $\alpha \cdot \mathbf{v} = \alpha\mathbf{v}$.

El ejemplo que motivó la definición fue $\mathbb{R}^n$ con las suma y mult. por escalar usuales. Vamos a demostrar que sí es un Esp. Vect.

Sobre $\mathbb{R}$:

4. Si $n \in \mathbb{N}$, el producto cartesiano $\mathbb{R}^n$ es un espacio vectorial, sobre $\mathbb{R}$ con las operaciones puntuales. Esto es,

$$+ : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n \text{ dada por } \quad (x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_n, \dots, x_n + y_n),$$

con neutro $\mathbf{0} = (0, 0, \dots, 0) \in \mathbb{F}^n$, y

$$\cdot : \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n \text{ dada por } \quad \alpha \cdot (x_1, \dots, x_n) = (\alpha x_1, \dots, \alpha x_n).$$

Se puede demostrar que $(\mathbb{F}^n, +, \cdot)$ es un espacio vectorial sobre $\mathbb{R}$.

Obs. Si V es esp. vect. sobre $\mathbb{F}$, también se usa la expresión

V es un $\mathbb{F}$-esp. vect. ($\mathbb{F}$-e.v.)

significa lo mismo.

Dem.

1] $(\mathbb{R}^n, \hat{+}, 0)$ es un gpo abeliano.

- Veamos que la suma es asociativa: Si $(x_1, \dots, x_n), (y_1, \dots, y_n)$ y $(z_1, \dots, z_n)$ son vectores en $\mathbb{R}^n$, ent.

$$\begin{aligned}
\big((x_1, \dots, x_n) \hat{+} (y_1, \dots, y_n)\big) \hat{+} (z_1, \dots, z_n) &= (x_1 + y_1, \dots, x_n + y_n) \hat{+} (z_1, \dots, z_n) \\
&= \big((x_1 + y_1) + z_1, \dots, (x_n + y_n) + z_n\big) \\
&= \big(x_1 + (y_1 + z_1), \dots, x_n + (y_n + z_n)\big) \\
&= (x_1, \dots, x_n) \hat{+} (y_1 + z_1, \dots, y_n + z_n) \\
&= (x_1, \dots, x_n) \hat{+} \big((y_1, \dots, y_n) \hat{+} (z_1, \dots, z_n)\big)
\end{aligned}$$

Def de $\hat{+}$ en $\mathbb{R}^n$

La suma en $\mathbb{R}$ es asociativa

Def de $\hat{+}$ en $\mathbb{R}^n$

$\Rightarrow$ La suma vectorial, $\hat{+}$, es asociativa.

- Demostrar que $\bar{0} = (0, \dots, 0)$ es el neutro de $\hat{+}$.
- Existencia de inversas: Si $(x_1, \dots, x_n) \in \mathbb{R}^n$, ent. el vector $(-x_1, \dots, -x_n)$ resulta ser el inverso aditivo de $(x_1, \dots, x_n)$.

En efecto:

$$(x_1,\dots,x_n)\,\hat{+}\,(-x_1,\dots,-x_n)=(x_1+(-x_1),\dots,x_n+(-x_n))$$

En $\mathbb{R}$, la suma tiene inversos

$$=(0,\dots,0).$$

- La conmutatividad de la suma: Sean $(x_1,\dots,x_n),(y_1,\dots,y_n)\in\mathbb{R}^n$.

Entonces

$$(x_1,\dots,x_n)\,\hat{+}\,(y_1,\dots,y_n)=(x_1+y_1,\dots,x_n+y_n)$$

La suma en $\mathbb{R}$ es conmutativa

$$=(y_1+x_1,\dots,y_n+x_n)$$

$$=(y_1,\dots,y_n)\,\hat{+}\,(x_1,\dots,x_n).$$

$\therefore\ (\mathbb{R}^n,\hat{+},\bar{0})$ es grupo abeliano.

Falta ver que $\cdot:\mathbb{R}\times\mathbb{R}^n\to\mathbb{R}^n$ cumple las propiedades correspondientes.

Asociatividad: Sean $\alpha,\beta\in\mathbb{R}$ y $(x_1,\dots,x_n)\in\mathbb{R}^n$. Ent.

$$\alpha\cdot(\beta\cdot(x_1,\dots,x_n))=\alpha\cdot((\beta x_1,\dots,\beta x_n))$$

Def. de $\cdot$ en $\mathbb{R}^n$

$$=(\alpha(\beta x_1),\dots,\alpha(\beta x_n))$$

El producto en $\mathbb{R}$ es asociativo

$$=((\alpha\beta)x_1,\dots,(\alpha\beta)x_n)$$

Def. de $\cdot$ en $\mathbb{R}^n$

$$=(\alpha\beta)\cdot(x_1,\dots,x_n)$$

Identidad: Sean $1\in\mathbb{R}$ el neutro mult. y $(x_1,\dots,x_n)\in\mathbb{R}^n$. Ent

$$1\cdot(x_1,\dots,x_n)=(1\cdot x_1,\dots,1\cdot x_n)=(x_1,\dots,x_n)$$

porque 1 es neutro mult. en $\mathbb{R}$

Distributividades derecha e izq: Son ejercicio.

De todo lo anterior, $(\mathbb{R}^n,\hat{+},\cdot)$ es un $\mathbb{R}$-esp. vect. $\blacksquare$