Práctica 0 - Estructuras algebraicas (o "Previously, on Algebra I....")

Departamento de Física - UNLP

Ej. 1 — Demuestre que el conjunto de los números enteros con la suma usual forman una estructura de grupo abeliano, pero que no lo hace con el producto.

Ej. 2 — Demuestre que el conjunto de las raíces $n-$ésimas de la unidad $W_n := \{z/z \in \mathbb{C}\ ; z^n = 1\}$ representa una estructura de grupo abeliano con el producto usual de números complejos. Construya la "tabla de multiplicar" de W_3.

Ej. 3 — Considere los anillos de enteros[1] $\mathbb{Z}_q$.

- Construya la tabla de sumar de $\mathbb{Z}_3$ y $\mathbb{Z}_4$ y verifique que respetan estructura de grupo.
- Construya la tabla de multiplicar de $\mathbb{Z}_3$ y $\mathbb{Z}_4$ y observe en qué caso se cumple que corresponda a un grupo.
- Probar que en general $\mathbb{Z}_q$ forma estructura de grupo con la $+$
- Usando el "pequeño teorema de Fermat" y el hecho de que el neutro de un grupo siempre es único, demuestre que estos conjuntos también forman una estructura de grupo con la multiplicación $\Leftrightarrow q$ es primo [2]. Verifique que en ese caso también se cumple que los $\mathbb{Z}_q$ tienen estructura de cuerpo con $+, *$.

Ej. 4 — Grupos de matrices:

- Demuestre que el conjunto de las matrices $\mathbb{R}^{n\times m}$ (con m y n fijos) forma una estructura de grupo con la suma usual de matrices.
- Demuestre que el conjunto *general lineal*($GL(n) : \{M/M \in \mathbb{R}^{n\times n}\ ; \det(M) \neq 0\}$) forma una estructura de grupo con el producto de matrices.
- Demuestre que el conjunto de las *matrices ortogonales* $O(n) : \{M/M \in \mathbb{R}^{n\times n}\ ; M^{\mathrm{t}}.M = I\}$ forma una estructura de grupo con el producto de matrices.
- Demuestre que el conjunto de las *matrices unitarias* $U(n) : \{M/M \in \mathbb{C}^{n\times n}\ ; M^{\dagger}M = I\}$ forma una estructura de grupo con el producto de matrices.
- Demuestre que el conjunto *especial* de las *matrices unitarias* $SU(n) : \{M/M \in U(n)\ ; \det(M) = 1\}$ forma una estructura de grupo con el producto de matrices.
- Demuestre que el conjunto de las matrices *hermíticas* invertibles en $\mathbb{C}^{2\times 2}$ $H(2) : \{M/M \in \mathbb{C}^{2\times 2}\ ; M = M^{\dagger}\ ; \det(M) \neq 0\}$ *NO* forma una estructura de grupo con el producto de matrices.

Ej. 5 — Grupos de simetría (opcional):

- Argumente (cualitativamente) que las traslaciones en el plano ($\mathbb{R}^2$) tienen estructura de grupo abeliano respecto al producto definido por la composición de translaciones (si T_1 y T_2 son traslaciones, $T_1 * T_2$ es la traslación que se obtiene de realizar primero T_2 y luego T_1).
- Argumente (cualitativamente) que el conjunto de las rotaciones discretas que transforman un triángulo equilátero en el mismo triángulo forman una estructura de grupo respecto al producto definido por la composición de rotaciones (si R_1, R_2 son rotaciones, $R_1 * R_2$ es la rotación que se obtiene de realizar primero R_2 y luego R_1). Asumiendo que dos rotaciones son equivalentes si llevan los tres vértices del triángulo a los mismos tres vértices, muestre que sólo existen tres rotaciones no equivalentes. Construya la tabla de multiplicar, y compare con las correspondientes tablas de multiplicar de W_3 (2) y $\mathbb{Z}_3$ (3) ¿Qué tienen en común?
- Argumente (cualitativamente) que las rotaciones en el *plano euclideo*($\mathbb{R}^2$) tienen estructura de grupo abeliano respecto al producto definido por la composición de rotaciones (como en el item anterior).
- Argumente (cualitativamente) que las rotaciones en el *espacio euclideo* ($\mathbb{R}^3$) tienen estructura de grupo respecto al producto definido por la composición de rotaciones, pero que ya no se trata de un grupo abeliano.

[1] $\mathbb{Z}_q = \{n\ /\ 0 \leq n < q\}$ con la suma y el producto definidos de manera que $a + b = c$ (mod q) y $a * b = d$ (mod q), donde (mod q) significa que c, d son números en $\mathbb{Z}_q$ tales que $a + b - c$ y $a * b - d$ tienen resto 0 en la división por q respectivamente

[2] El pequeño teorema de Fermat establece que si q es un número primo $\forall a \in \mathbb{Z}_q$, $a^q = a$(mod q)