Ayudantía 1 Estructuras Algebraicas MAT214

Universidad Técnica Federico Santa María

11 de marzo de 2019

1. Sea $\mathcal{R}$ una relación de equivalencia en un conjunto A, demuestre que:
   a) $\forall\ a \in A,\ a \in [a]_{\mathcal{R}}$
   b) Si $b \in [a]_{\mathcal{R}}$ entonces $a \in [b]_{\mathcal{R}}$ y además $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$
   c) $\forall\ a, b \in A$, $[a]_{\mathcal{R}} = [b]_{\mathcal{R}}$ o bien $[a]_{\mathcal{R}} \cap [b]_{\mathcal{R}} = \emptyset$.

2. a) Demuestre que la división euclídea implica que:
   $$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \cdots, [n-1]_n\}$$
   b) Demuestre que $\forall\ a, b \in \mathbb{Z}$ se tiene que $[a+b]_n$ y $[a \cdot b]_n$ solo dependen de la clase y no del representante elegido, i.e. si $a \equiv a'(\text{mod n})$ y $b \equiv b'(\text{mod n})$ entonces $[a+b]_n = [a'+b']_n$ y $[a \cdot b]_n = [a' \cdot b']_n$.

3. Sea G un grupo tal que $g^2 = e$, $\forall g \in G$. Demuestre que G es abeliano.

4. Demuestre que los subgrupos de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$ con $n \in \mathbb{Z}$.

5. Sea $f : G \to G'$ un morfismo sobreyectivo. Demuestre que si G es abeliano, entonces G' es abeliano y que si G es cíclico entonces G' es cíclico.

6. Sea G un grupo finito tal que existe p primo que divide a $|G|$, demuestre que existe un elemento en G de orden p. Para demostrar esto, se define a $\mathcal{S}$ como el conjunto:
   $$\mathcal{S} = \{(x_1, \cdots, x_p) \mid x_i \in G \text{ y } x_1 x_2 \cdots x_p = e\}$$
   a) Muestre que $\mathcal{S}$ tiene $|G|^{p-1}$ elementos.
   Defina la relación $\sim$ en $\mathcal{S}$ como $a \sim b \iff b$ es una permutación cíclica de a.
   b) Pruebe que la permutación cíclica de un elemento de $\mathcal{S}$ sigue estando en $\mathcal{S}$.
   c) Pruebe que $\sim$ es una relación de equivalencia en $\mathcal{S}$.
   d) Pruebe que una clase de equivalencia contiene un único elemento si y solamente si es de la forma $(x, \cdots, x)$ con $x^p = e$.
   e) Pruebe que cada clase de equivalencia tiene orden 1 o p. Deduzca que $|G|^{p-1} = k + pd$, donde k es el número de clases de tamaño 1 y d es el número de clases de tamaño p.
   f) Dado que $\{(e, \cdots, e)\}$ es una clase de equivalencia, por el enunciado (e) concluya que debe haber un elemento $x \in G$ distinto de e tal que $x^p = e$.

7. Usando el Teorema de Lagrange en el grupo multiplicativo $(\mathbb{Z}/p\mathbb{Z})^{\times}$ demuestre que si p es un número primo, entonces $a^p \equiv a(\text{mod p})$ para todo $a \in \mathbb{Z}$.