Introducción a las Estructuras Algebraicas
Tarea 2

Prof. Mauricio Medina

1. Sea A un conjunto no vacío y sea $F(A) = \{f : A \to A \mid f \text{ es función biyectiva}\}$. Demuestre que $F(A)$ es un grupo con la composición de funciones.

2. Sea A un conjunto no vacío. Demuestre que $(\mathcal{P}(A), \triangle, \cap)$ es un anillo conmutativo con uno, donde $X \triangle Y = (X \cup Y) - (A \cap B)$.

3. Demuestre que el producto en $\mathbb{Z}$ es asociativo.

4. Demuestre que el subconjunto $\mathbb{Z}^+$ es cerrado bajo el producto.

5. Demuestre que $\mathbb{Z}^+ = \mathbb{N}$. (Viendo a $\mathbb{N}$ dentro de $\mathbb{Z}$)

6. Sean $a, b \in \mathbb{Z}$. Definimos al relación siguiente:

$$a \leq b \;\Leftrightarrow\; a = b \;\text{ ó }\; b - a \in \mathbb{Z}^+$$

   Demuestre que $\leq$ es un orden parcial en $\mathbb{Z}$.

7. Pruebe que si $0 \neq a \in \mathbb{Z}$, entonces $a^2 > 0$.

8. Pruebe que si $a, b \in \mathbb{Z}$ con $a < b$, entonces $-a > -b$.

   Def. Sea $(R, +\cdot)$ un anillo con uno y $u \in A$. Decimos que u es una unidad si u tiene inverso multiplicativo, i.e., existe $v \in R$ tal que $uv = 1 = vu$.

9. Demuestre que las unidades de $\mathbb{Z}$ son 1 y -1.

   Def. Sea $a \in \mathbb{Z}$. El valor absoluto de a, denotado como $|a|$ es definido de la siguiente manera:

$$|a| = \begin{cases} a \text{ si } a \geq 0 \\ -a \text{ si } a < 0 \end{cases}$$

10. Demuestre que el valor absoluto satisface las siguientes propiedades:

    a) Para todo $a \in \mathbb{Z}$, $|a| = |-a|$.
    b) Para todo $a \in \mathbb{Z}$, $|a| \geq 0$, más aún, $|a| = 0$ si y solo si $a = 0$.
    c) Para todo $a \in \mathbb{Z}$, $\pm a \leq |a|$.
    d) Para todo $a, b \in \mathbb{Z}$, $|ab| = |a||b|$.

e) Para todo $a, b \in \mathbb{Z}$, $|a+b| \leq |a| + |b|$. (Desigualdad del triangulo)

11. Demuestre que si $a|b$ entonces $a|-b$, $-a|b$ y $-a|-b$.

12. Demuestre que si $a|1$ entonces $a = \pm 1$.

13. Demuestre que si $a|b$ y $b|a$ entonces $a = \pm b$.

14. Demuestre que si $a|b$ y $b \neq 0$, entonces $|a| \leq |b|$.

15. Use inducción sobre n para probar que si $a|b_1, a|b_2, ..., a|b_n$ y $r_1, ..., r_n \in \mathbb{Z}$, entonces $a|r_1b_1 + r_2b_2 + \cdots + r_nb_n$.

16. Si $a \neq 0$, demustre que $mcd(a, 0) = |a|$.

17. Sea $a, b \in \mathbb{Z}$ y $d = mcd(a, b)$. Si $a = da'$ y $b = db'$ demuestre que $mcd(a', b') = 1$.

    Def. Cuando dos enteros tienen máximo común divisor igual a 1, decimos que estos enteros son primos relativos.

18. Demuestre que dos enteros consecutivos son primos relativos.

19. Demuestre que para todo $r \in \mathbb{Z}$, se tiene que $mcd(a, b + ar) = mcd(a, b)$.

20. Demuestre que para todo $c \geq 1$, se tiene que $mcd(ca, cb) = c(mcd(a, b))$.

21. Usando el algoritmo de Euclides calcule los siguientes maximos comunes divisores y expreselos en combinación lineal.

    - $mcd(2947, 3997)$
    - $mcd(329, 1005)$
    - $mcd(7469, 2464)$
    - $mcd(1109, 4999)$
    - $mcd(1819, 3558)$