Universidad del Istmo de Guatemala
Facultad de Ingenieria
Ing. en Sistemas
Informatica 1
Prof. Ernesto Rodriguez - erodriguez@unis.edu.gt

Hoja de trabajo #9

Fecha de entrega: 8 de Octubre, 2019 - 11:59pm

Instrucciones: Resolver cada uno de los ejercicios siguiendo sus respectivas instrucciones. El trabajo debe ser entregado a traves de Github, en su repositorio del curso, colocado en una carpeta llamada "Laboratorio 9". Al menos que la pregunta indique diferente, todas las respuestas a preguntas escritas deben presentarse en un documento formato pdf, el cual haya sido generado mediante Latex.

Nota: Para esta tarea, debe tener instalado "Elm" en su computadora. Puede obtener el lenguaje "Elm" en: https://guide.elm-lang.org/install.html

Ejercicio #1 (20%)

Defina un *tipo generico* llamado **Grupo**. Este tipo debe tener los siguientes constructores:

- **Valor** : $`t \rightarrow$ (**Grupo** $`t)$
- **Suma** : (**Grupo** $`t) \rightarrow$ (**Grupo** $`t) \rightarrow$ (**Grupo** $`t)$
- **Inverso** : (**Grupo** $'t) \rightarrow$ (**Grupo** $`t')$

Ejercicio #2 (20%)

Defina un *tipo generico* llamado **Algebra** $`t$ $`s$. Este tipo solamente tiene un constructor:

- **Algebra** : $(`t \rightarrow `s) \rightarrow (`s \rightarrow `s \rightarrow `s) \rightarrow (`s \rightarrow `s) \rightarrow$ **Algebra**

A este tipo se le referira como el *algebra de* **Grupo**. El proposito de este tipo es especificar como se debe interpretar un valor de tipo **Grupo**. Funciona de forma similar a un *fold* ya que su primer parametro corresponde al constructor **Grupo**, su segundo parametro al constructor **Suma** y su tercer parametro al constructor **Inverso**.

Ejercicio #3 (20%)

Definir una función llamada "`evaluar` : **Algebra** $`t$ $`s \rightarrow$ **Grupo** $`t \rightarrow `s$". El proposito de esta funcion es evaluar un **Grupo** y obtener el resultado final al evaluar un gruop utilizando el algebra proporcionado. Esta función debe operar de la siguiente manera:

- Si el **Grupo** es un **Valor**, utilizar la primera función del algebra para convertir el valor a un valor de tipo $`a$
- Si el **Grupo** es una **Suma**, llamar recurisvamente la funcion `evaluar` con cada uno de los parametros de la **Suma** y luego obtener el resultado final evaluando los dos valores obtenidos anteriormente con la segunda función del `Algebra`
- Si el **Grupo** es un **Inverso**, evaluar recurisvamente el parametro de **Inverso**. Luego utilizar la tercera función del **Algebra** para obtener el resultado final

Ejercicio #4 (40%)

El *grupo* $\mathbb{Z}^n$ donde n es primo, es un grupo comunmente utilizado en la criptografia y otras aplicaciones de la computación (`https://www.youtube.com/watch?v=kpk2tdsPh0A`). Este grupo esta formado por los numeros $0 \ldots (n-1)$, en otras palabras, todos los numeros enteros empezando en cero y terminando en $n-1$. La suma en $\mathbb{Z}^n$ funciona exactamente igual que la suma tradicional excepto que al resultado siempre se le aplica la función `modulo` con base n (residuo del resultado al dividirlo dentro de n). Tomemos como ejemplo el grupo $\mathbb{Z}^5$ y las siguientes operaciónes:

- $1 + 3 = 4$ (**modulo** 5) $= 4$
- $2 + 3 = 5$ (**modulo** 5) $= 0$
- $3 + 4 = 7$ (**modulo** 5) $= 2$

En otras palabras, los valores producidos al sumar los numeros siempre se colocan en el rango $[0, 5)$ (ya que $n = 5$).

El inverso de un grupo es un valor llamado $a^(-1)$ (para todo a) tal que se cumple la siguiente propiedad: $\forall\, a, b \in \mathbb{Z}^n \,.\, a + b + a^{-1} = b$ en otras palabras, el valor a^{-1} "invierte" el efecto causado por operar a. En los numeros enteros ($\mathbb{Z}$), el inverso de un numero es el negativo de dicho numero. Sin embargo, en el grupo $\mathbb{Z}$ no existen los negativos. A pesar de ello si existe el inverso. Tome como ejemplo $\mathbb{Z}^5$:

- $(3 + 2) + 2 = 7$ (**modulo** 5)=2
- $(3 + 4) + 2 = 9$ (**modulo** 5)=4
- $(3 + 5) + 2 = 10$ (**modulo** 5) $= 5$

En otras palabras, para el grupo $\mathbb{Z}^5$, el *inverso* de 3 es 2 ya que este valor hace que la operación entre 3 y otro numero resulte en el numero que fue operado.

Su tarea es utilizar este conocimiento para implementar una función llamada `zAlgebra` : **Int** $\rightarrow$ **Algebra Int Int**. El primer parametro de esta función es el valor n y el algebra retornada debe cumplir con las reglas mencionadas anteriormente. Asegurese de probar que su algebra funcione correctamente. Por ejemplo, la siguiente expresión:

`evaluar` (`zAlgebra 5`) (**Suma** 3 (**Suma** 5 (**Inverso** 3)))

Produciria 5 como resultado.