Problem Set 9

Deliverable: Submit your responses as a single, readable PDF file on the collab site before **6:29pm** on **Friday, 1 December**.

Collaboration Policy - Collaboration Policy (identical to PS5)

For this assignment, you may work in groups of one to three students to write-up a solution together. If you work with teammates, exactly one of you should submit one assignment that represents your collective best work with all of your names and UVA ids clearly marked on it on it. *Everyone on a team should understand everything you turn in for the assignment well enough to be able to produce it completely on your own.* All teammates must review the submissions before it is submitted to make sure you understand everything on it and that your name and UVA id are clearly marked on it.

Preparation

This problem set focuses on number theory — Chapter 9 of the MCS book, and Class 20, Class 22, and Class 23.

Directions

Solve all [TODO] problems. Your answers should be clear, consise, and convincing.

Abelian Groups

For each set (R) and operator (P) described below, explain why it is not an Abelian group (defined in Class 22). Your answer should include a convincing supporting argument that shows why the given set and operator do not satisfy at least one of the required properties.

1. $R = \mathbb{Z}, P =$ gcd where gcd is a binary operator that takes two integers as input and outputs their greatest common divisor.
2. $R = \mathbb{Z}, P = -$.
3. $R = \{T, F\}, P =$ OR. (Hint: what must the identity be, and which element has no inverse?)

Fields

For each set (R) and first and second operations (P_+, $P_\times$), answer if the set and operations are a *field* (as defined in Class 23). A good answer will either show how the given set and operations satisfy the required properties (including explaning what the additive identify and multiplicative identity are), or show how it fails to satisfy one of the required properties.

4. $R = \mathbb{N}_1 2, P_+ = +(\text{mod} 12), P_\times = \times(\text{mod} 12)$.
5. $R = \{\sharp, \flat\}, P_+ = \{(\sharp, \sharp) \to \sharp, (\sharp, \flat) \to \flat, (\flat, \sharp) \to \flat, (\flat, \flat) \to \sharp\}, P_\times = \{(\sharp, \sharp) \to \sharp, (\sharp, \flat) \to \sharp, (\flat, \sharp) \to \sharp, (\flat, \flat) \to \flat\}$.
6. $R = \mathbb{N}_3 1, P_+ = \times(\text{mod} 31), P_\times = +(\text{mod} 31)$.

