Math-113, Homework 8, non textbook problems

A. Let A be an abelian group. Denote by

$$\mathcal{H} = \{\phi : A \to A \mid \phi \text{ is a group homomorphism}\}$$

the collection of all homomorphisms from A to itself. Define two binary operations $+, * : \mathcal{H} \times \mathcal{H} \to \mathcal{H}$ as follows: For each $f, g \in \mathcal{H}$

$$(f+g) : A \to A, \qquad (f+g)(a) = f(a) + g(a) \tag{1a}$$
$$(f*g) : A \to A, \qquad (f*g)(a) = f(g(a)) \tag{1b}$$

- Prove that both operations are well-defined, namely that $f+g$ and $f*g$ are always group homomorphisms.
- Prove that $(\mathcal{H}, +, *)$ is a ring.
- Is it a division ring? Prove or provide a counterexample.

Remark 1: The above ring is called the *endomorphism* ring of A and denoted by $End(A)$. A well known example of such rings comes from linear algebra, when A is a vector space (which is an abelian group w.r.t. addition).

B. Let A be an abelian group. Now let

$$\mathcal{F} = \{f : A \to A\}$$

be the collection of all maps from A to itself. Define binary operations $+, * : \mathcal{F} \times \mathcal{F} \to \mathcal{F}$ as in (1).

- Prove that (R1) is satisfied, i.e. that $(\mathcal{F}, +)$ is an Abelian group. What is an identity of $(\mathcal{F}, +)$?
- Prove that (R2) is satisfied, i.e. that $(\mathcal{F}, *)$ is associative.
- Exactly one of the two distributive laws in (R3) fails in general. Determine which distributive law (left or right) holds for $(\mathcal{F}, +, *)$. Prove one distributive law and provide a counterexample to the other.

C. Consider the set of complex integers

$$\mathbb{Z}[\mathbf{i}] = \{n + m\mathbf{i} \mid n, m \in \mathbb{Z}\} \qquad \subset \quad \mathbb{C}$$

- Prove that $\mathbb{Z}[i]$ is a ring. This ring is called the *Gaussian Integers.*
- Prove that the group of units

  $$(\mathbb{Z}[\mathbf{i}])^{\times} = \{1, -1, \mathbf{i}, -\mathbf{i}\}$$

  has exactly four elements.
  Hint: Recall from HW1 how $|x + \mathbf{i}y| = \sqrt{x^2 + y^2}$ *behaves w.r.t. multiplication of complex numbers.*
- Is the group of units $((\mathbb{Z}[\mathbf{i}])^{\times}, \times)$ abelian? Determine its isomorphism class.
- Prove that $1 + \mathbf{i}$ is a "Gaussian prime", namely that whenever for $a, b \in \mathbb{Z}[\mathbf{i}]$

  $$ab = 1 + \mathbf{i} \qquad \Leftrightarrow \qquad \text{either } a \text{ is a unit, or } b \text{ is a unit.}$$

D.(Not for the grade)

Note that the group of units in integers is $\mathbb{Z}^{\times} = \{1, -1\} \simeq \mathbb{Z}_2$, similarly $(\mathbb{Z}[\mathbf{i}])^{\times} = \{1, -1, \mathbf{i}, -\mathbf{i}\} = \ldots$. What will be the group of units for integer quaternions?