Homework Ten

In anticipation of your midterm, which will be more difficult than the first (but you will have more time for it), this homework is a bit harder. As usual, parts and problems with * need not be turned in.

1. Fields are very simple

Show that a commutative ring R is a field if and only if it only has two ideals: $\{0\}$ and R itself.

REMARK 1.1. In other words, there are no meaningful quotient rings you can make out of fields—there simply aren't any interesting ideals to quotient by. So in terms of being indecomposable, this means fields are like simple groups. When one tries to use the algebra of commutative rings to study spaces, this is the reason that fields will often play the role of "points"—they are spaces that cannot be decomposed any further.

2. Maximal ideals and fields

An ideal $I \subset R$ of a commutative ring is called *maximal* if the only ideal containing I is R or I itself.

(a) If I is a maximal ideal, prove that R/I is a field.
(b) * Prove the converse. You may want to prove a lemma that ideals in R containing I are in bijection with ideals in R/I.
(c) Prove that $n\mathbb{Z} \subset \mathbb{Z}$ is maximal if and only if n is a prime. (Hint: Any ideal must in particular be a subgroup of $\mathbb{Z}$, and you know what all subgroups of $\mathbb{Z}$ look like.) You have shown that $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime.
(d) In $\mathbb{Z}/7\mathbb{Z}$, verify that $\mathbb{Z}/7\mathbb{Z} - \{\overline{0}\}$ is a group by writing out its multiplication table. How does your table show that it's a group?

3. Field of order 4

From above, we learned that there is a field of order p for any prime number p. It turns out there is a field of order p^k for any prime p and any

positive integer $k \geq 1$. We probably won't be able to prove it, except now, when $p^k = 4$.

(a) Exhibit a field $\mathbb{F}_4$ of order 4. Trial and error may be inevitable. As a hint, $\mathbb{F}_4$ is not isomorphic to $\mathbb{Z}/4\mathbb{Z}$ as an abelian group.
(b) Let $\mathbb{F}_8$ be a field of 8 elements. (Assume it exists.) Why is $(\mathbb{F}_8 - \{0\}, \times)$ cyclic?

4. Direct sum modules and quotient modules

Fix a ring R. We'll set up the idea of quotient modules and product modules, the same way we did for groups.

(a) Show that the functions

$$M \to M \oplus N, \qquad m \mapsto (m, 0) \qquad \text{and} \qquad M \oplus N \to M, \qquad (m, n) \mapsto m$$

are both left R-module homomorphisms.
(b) Let $f : M \to N$ be a homomorphism of left R-modules. Let the kernel and image of f be the kernel and image of f as a group homomorphism. Show both $ker(f) \subset M$ and $im(f) \subset N$ are submodules.
(c) Let $M' \subset M$ be a submodule, and let M/M' be the quotient abelian group. Show that the action

$$R \times M/M' \to M/M', \qquad r\overline{x} := \overline{rx}$$

makes M/M' into a left R-module.
(d) Let M and N be left R-modules. Show that $\hom_R(M, N)$ is an R-module under the addition where if $f, g \in \hom_R(M, N)$, then $f + g$ is defined via

$$(f + g)(x) = f(x) + g(x)$$

and for $r \in R$, the function rf is defined via

$$(rf)(x) = r(f(x)).$$

Here, x is any element of M.

5. The Hamiltonians/Quaternions

We all know $\mathbb{R}^4$ is a vector space. Using an identification $\mathbb{R}^4 \cong \mathbb{R} \times \mathbb{R}^3$, let us write an element of $\mathbb{R}^4$ as

$$(t, \vec{v}) \in \mathbb{R} \times \mathbb{R}^3.$$

For historical reasons, we will write $\mathbb{H}$ instead of $\mathbb{R}^4$ in what follows.

Define a function

$$\mathbb{H} \times \mathbb{H} \to \mathbb{H}$$

by the formula

$$(s, \vec{u})(t, \vec{v}) := (st - \vec{u} \cdot \vec{v}, s\vec{v} + t\vec{u} + \vec{u} \times \vec{v}).$$

Here, $\cdot$ is the dot product for $\mathbb{R}^3$ and $\times$ is the cross product for $\mathbb{R}^3$.

In the following proofs, I strongly encourage you to never write out the components of $\vec{u} \in \mathbb{R}^3$. I remind you that you don't need to turn in the problems with asterisks.

(a) * Prove that the multiplication above is associative. Verifying associativity requires a lot of terms, so be organized!
(b) * Prove that multiplication distributes over addition of vectors.
(c) Prove that $1 := (1, (0, 0, 0))$ is the multiplicative unit.
(d) Prove by example that multiplication is not commutative.
(e) Let

$$i := (0, (1, 0, 0)), \qquad j := (0, (0, 1, 0)), \qquad k := (0, (0, 0, 1)).$$

Prove that these all square to the element

$$-1 := (-1, (0, 0, 0)) \in \mathbb{H}.$$

(f) Given an element $x = (t, \vec{v})$, let $|x|^2$ equal the usual norm-squared of a vector, so

$$|x|^2 = t^2 + |v|^2.$$

Show that $|xy| = |x||y|$. In other words, multiplication preserves the norm.
(g) Given an element $x = (t, \vec{v})$, let $\overline{x}$ denote the element $(t, -\vec{v})$. Show that any non-zero element x has a multiplicative inverse given by $\overline{x}/|x|^2$.

REMARK 5.1. This ring is often called the *Hamiltonians*, or the *Quaternions*. As you proved above, it has the property that $\mathbb{H} - \{0\}$ is a group, but this ring is not a field. This is because the multiplication is not commutative. Such rings are called *skew fields*. When one does not demand that $R - \{0\}$ is a group, but that every non-zero element has an inverse, R is called a *division rings*.

REMARK 5.2. You might ask, how many division rings are there? It turns out that every *finite* division ring must be a field. This is called Wedderburn's Little Theorem.

And how many division rings are there that contain the field $\mathbb{R}$ inside of them? Not many–it turns out that there are only *four* division rings that are vector spaces over $\mathbb{R}$:

(1) the ring with a single element, which is the zero ring.
(2) The ring $\mathbb{R}$,
(3) The ring $\mathbb{C}$, and
(4) The ring $\mathbb{H}$.

This is called the *Frobenius Theorem*.

6. (*) $\mathbb{R}[t]/(t^2+1) \cong \mathbb{C}$

As usual, in what follows, $\overline{a}$ represents the equivalence class of $a \in R$ in the quotient ring R/I.

(a) Show that $\mathbb{R}[t]/(t^2+1)$ is a vector space over $\mathbb{R}$ with basis given by $\overline{1}$ and $\overline{t}$.
(b) Show that $\mathbb{C}$ is a vector space over $\mathbb{R}$ with basis given by 1 and i.
(c) Show that there is an $\mathbb{R}$-linear map $f : \mathbb{R}[t]/(t^2+1) \to \mathbb{C}$ sending $\overline{1} \mapsto 1$ and $\overline{t} \mapsto i$. Why must this be a bijection?
(d) Show that f is a ring isomorphism.
(e) Conclude that $\mathbb{R}[t]/(t^2+1)$ must be a field.

7. (*) Linear algebra, applied

Let V_d be the set of polynomials in t of degree $\leq d$ with $\mathbb{R}$ coefficients. Fix $d+1$ real numbers, $a_0, a_1, \ldots, a_d$. Consider the function

$$ev_{a_0,a_1,\ldots,a_d} : V_d \to \mathbb{R}^{d+1}$$

which sends a polynomial p to the column vector

$$\begin{bmatrix} p(a_0) \\ p(a_1) \\ \vdots \\ p(a_d) \end{bmatrix}$$

.

(a) Show that $ev_{a_0,a_1,\ldots,a_d}$ is an $\mathbb{R}$-linear map for any choice of real numbers $a_0, a_1, \ldots, a_d$.
(b) If each a_i is distinct, show that the linear map is an injection.
(c) What is the dimension of V_d?
(d) Prove that for any collection of distinct real numbers

$$(a_0, a_1, \ldots, a_d)$$

and any collection of real numbers

$$(z_0, \ldots, z_d)$$

there exists a unique polynomial p such that

$$p(a_i) = z_i.$$

(e) Fix a field F. Prove that for any collection of distinct elements

$$(a_0, a_1, \ldots, a_d), \qquad a_i \in F$$

and any collection of elements

$$(z_0, \ldots, z_d), \qquad z_i \in F$$

there exists a unique degree d polynomial p with coefficients in F such that

$$p(a_i) = z_i.$$