MA 341: Advanced Problems for Fun: # 1

We say that $\mathbb{Z}$ is an example of a ring, namely it has two operations $+$ and $\cdot$ which satisfy the "algebra axioms", i.e. are associative, commutative, satisfy the distributive law, and have the usual relations with 0 and 1. In this series of exercises, we will describe $\mathbb{Z}$ completely using only a short list of additional axioms.

1. We say that a ring R is *ordered* if there exists a non-empty subset $P \subseteq R$ satisfying the following:

   - $\forall a, b \in P, a + b \in P$ and $a \cdot b \in P$.
   - (Trichotomy) Exactly one of the following holds $\forall a \in R$: $a \in P, a = 0, -a \in P$.

   This set P is meant to model the positive integers in $\mathbb{Z}$, and is called the subset of positive elements of R. Show that $1 \in P$. Note if R is ordered, P need not be unique. (Can you think of an example[1]?)

2. If R is ordered with set P as above, show that the relation $a > b$ if $a - b \in P$ defines a total ordering on R.

3. Show that $a > b$ and $c > d$ implies $a + c > b + d$ in an ordered ring. Show if $c > 0$, then $a > b$ implies $a \cdot c > b \cdot c$. What if $c < 0$? Find a suitable definition for $a \geq b$ and prove analogous results. (Since P need not be unique, a choice of positive elements is implicitly made to use the notation $>$.)

4. Examples of ordered rings you know include: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ with their usual positive elements. Show that $\mathbb{Z}_m$, the integers mod m, is never ordered. In fact, no finite ring is ordered.

5. We can go further than the last exercise: show if $n \cdot 1 = 1 + 1 + \cdots + 1 = 0$ in R for some n, then R is not ordered. (This includes finite rings!)

6. Show that if a ring R contains an element x such that $x^2 = -1$, then R is not ordered.

7. Show if R is ordered, then $a \cdot b = 0$ implies $a = 0$ or $b = 0$.

8. A *ring homomorphism* is a function $f : R \to S$ between rings such that $f(a + b) = f(a) + f(b)$, $f(a \cdot b) = f(a) \cdot f(b)$, and $f(1) = 1$. Show that any ring homomorphism $f : \mathbb{R} \to \mathbb{R}$ has to preserve inequalities. Use this to show any ring isomorphism from $\mathbb{R}$ to $\mathbb{R}$ (i.e. a bijective homomorphism) has to be the identity function.

9. We say a ring is well-ordered if it is ordered and its subset of positive elements P satisfies the well-ordering principle: any non-empty subset $S \subseteq P$ has a smallest element. Show that if R is a well-ordered ring, then there exists (exactly one) ring isomorphism $f : \mathbb{Z} \to R$, and this takes the usual positive integers to the set P. We say that $\mathbb{Z}$ is the "unique well-ordered ring up to unique isomorphism."

[1] It may be a bit tricky how to make an example, but this isn't necessary for the rest of the set.

10. (Induction) The "principle of mathematical induction" is actually a feature about $\mathbb{Z}$. We say an ordered ring R has the "induction feature" (totally my own term) if its subset of positive elements P has the following property:

    - If $S \subseteq P$ with $1 \in S$ and $n \in S \implies (n+1) \in S$, then $S = P$.

    Show that any ordered ring R with the "induction feature" admits a unique isomorphism to $\mathbb{Z}$, and this isomorphism takes P to the positive integers. (Try writing an induction proof using this feature's wording!)

11. Throughout the course, we've used a lot of "basic facts" about how algebra works in $\mathbb{Z}$ in our proofs, right from the start. The exercises above prove some of these, but feel free to go back and check every manipulation we've done rests only on the assumption that $\mathbb{Z}$ is a well-ordered ring. In fact, every thing you know about $\mathbb{Z}$ should follow from these axioms. For example, there are no integers between n and $n+1$ for any $n \in \mathbb{Z}$. Can you prove it just from these axioms? Is it possible to prove this fact without using well-ordering?

12. (NIBZO) The last exercise establishes a dear fact you know about $\mathbb{Z}$: there are No Integers Between Zero and One, i.e. there are no $x \in \mathbb{Z}$ such that $0 < x < 1$. Suppose an ordered ring R has this property, that there are no $x \in R$ with $0 < x < 1$. Must there exist an isomorphism from $\mathbb{Z}$ to R?