Math 347H: Fundamental Math (H) HOMEWORK 5 **Due date: Oct 19 (Thu)**

1. Prove that multiplication is well-defined on $\mathbb{Q}$. Begin by stating exactly what you need to prove.

2. Prove that $(\mathbb{Q},+,\cdot)$ is a field by checking all of the required axioms one-by-one (even the ones proven in class).

3. Denote the elements (i.e. equivalence classes) in $\mathbb{Q}$ by $\left[\frac{a}{b}\right]$, omitting writing E in the superscript. An element $\left[\frac{a}{b}\right] \in \mathbb{Q}$ is said to be *positive* if a is positive. Define a binary relation $<$ on $\mathbb{Q}$ by setting, for each $\left[\frac{a}{b}\right], \left[\frac{c}{d}\right] \in \mathbb{Q}$,

$$\left[\frac{a}{b}\right] < \left[\frac{c}{d}\right] :\Leftrightarrow \left[\frac{c}{d}\right] - \left[\frac{a}{b}\right] \text{ is positive.}$$

(a) Prove that the notion of positivity is well-defined on $\mathbb{Q}$. Conclude that $<$ is well-defined.

(b) Prove that $<$ is a total strict order on $\mathbb{Q}$.

(c) Prove that $<$ satisfies Axioms (O3) and (O4) (written on page 12 of Sally's book).

This makes $\mathbb{Q}$ an *ordered field*.

4. For $n \geq 2$, show that for any $a, b \in \mathbb{Z}$, $a \equiv b \,(\mathrm{mod}\ n)$ if and only if $a - b$ is divisible by n.

5. Let $n \geq 2$ and consider the ring $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$. Prove that there is no binary relation $<$ that makes this ring an *ordered ring*, i.e. there is no total strict order $<$ on $\mathbb{Z}/n\mathbb{Z}$ satisfying Axioms (O3) and (O4).

6. Let $(R,+,\cdot)$ be a ring and let $0_R, 1_R$ denote its additive and multiplicative identities. Prove:

(a) The additive and the multiplicative identities are unique.

(b) Each $x \in R$ has a *unique* additive inverse.

(c) Each $x \in R$ has at most one multiplicative inverse.

(d) For each $x \in R$, $0_R \cdot x = 0_R = x \cdot 0_R$.

(e) If every nonzero[1] $x \in R$ has a multiplicative-inverse, then R satisfies the cancellation axiom, namely for all $x, y \in R$, if $x \cdot y = 0_R$ then $x = 0_R$ or $y = 0_R$. Thus, a field is a domain.
If $0_R = 1_R$ then R has only one element, namely, $R = \{0_R\}$. In this case, we call R the *zero ring* or the *trivial ring*.

7. Let $(R,+,\cdot)$ be a ring and let $0_R, 1_R$ denote its additive and multiplicative identities. A subset $R_0 \subseteq R$ is called a *subring* if $(R_0,+,\cdot)$ is a ring. Recall that, unlike the textbook, our definition of ring includes the existence of multiplicative identity; in particular, R_0

[1] Not equal to 0_R.

should have both additive and multiplicative identities, by definition; denote them by 0_{R_0} and 1_{R_0}, respectively.

(a) Prove that for a subring $R_0 \subseteq R$, $0_{R_0} = 0_R$ and $1_{R_0} = 1_R$.

(b) For a subset $R_0 \subseteq R$, prove that R_0 is a subring if and only if $R_0 \ni 1_R$ and for all $a, b \in R_0$, the elements $a - b$ and $a \cdot b$ are also in R_0.

(c) Show by example that a subring of a field need not be a field.