**MATH 4000/6000 – Homework #4**

posted February 27, 2024; due March 1, 2024 by 5 PM

You did a number on me. But, honestly, baby, who's counting?
— Taylor Swift

Assignments are expected to be neat and stapled. **Illegible work may not be marked**. Starred problems (*) are required for those in MATH 6000 and extra credit for those in MATH 4000.

1. Let $R$ be a ring, and let $R'$ be a subset of $R$. We call $R'$ a **subring** of $R$ if
   (A) $R'$ is a ring for the same operations $+$ and $\cdot$ as in $R$, *and*
   (B) $R'$ contains the multiplicative identity $1_R$ of $R$.

   (For example, making the identification discussed in class, $\mathbb{Z}$ is a subring of $\mathbb{Q}$.)

   (a) Let $R$ be a ring. Suppose that $R'$ is a subset of $R$ closed under the $+$ and $\cdot$ operations of $R$, that $R'$ contains the additive inverse (in $R$) of each of its elements, and that $R'$ contains $1_R$. Show that $R'$ is a subring of $R$.

   *Hint.* (B) holds by assumption. Check that all the ring axioms hold for $R'$ in order to verify (A). To get started, show that $0_R$ must belong to $R'$.

   (b) Find a two-element subset $R'$ of $R = \mathbb{Z}_6$ that satisfies condition (A) in the definition of a subring but not (B). You do **not** have to give a detailed proof that (A) holds.

2. (Introduction to the Gaussian integers) Let $\mathbb{Z}[i]$ be the subset of complex numbers defined by $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

   (a) Check that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$. (Exercise 1 above may be helpful.)

   (b) Define a function $N\colon \mathbb{Z}[i] \to \mathbb{R}$ by $N(z) = z \cdot \bar{z}$. This is called the **norm** of $z$. Explain why $N(z)$ is a nonnegative integer for every $z \in \mathbb{Z}[i]$. For which $z \in \mathbb{Z}[i]$ is $N(z) = 0$?

   (c) Prove that $N(zw) = N(z)N(w)$ for all $z, w \in \mathbb{Z}[i]$.

   (d) Using (c), show that $z \in \mathbb{Z}[i]$ is a unit $\iff N(z) = 1$. Then find (with proof) all units in $\mathbb{Z}[i]$.

3. Let $F$ be a field in which $1 + 1 \neq 0$, and let $a$ be a nonzero element of $F$. Show that the equation $z^2 = a$ has either no solutions in $F$ or exactly two distinct solutions.

   *Hint.* If $z_1^2 = a$ and $z_2^2 = a$, how are $z_1$ and $z_2$ related?

4. (Quadratic Formula!) Let $F$ be a field with $1 + 1 \neq 0$. Suppose $f(x) \in F[x]$ has degree 2, and write $f(x) = ax^2 + bx + c$, where $a, b, c \in F$. Define $\Delta$ by setting $\Delta = b^2 - 4ac$.

   (a) Show that if $R$ is an element of $F$ with $R^2 = \Delta$, then

   $$\frac{-b + R}{2a}$$

   is a root of $f$ that belongs to $F$. (Interpret the fraction $\frac{-b+R}{2a}$ as $(-b + R)(2a)^{-1}$, which makes sense as an element of of $F$ because $2a$ is a nonzero element of $F$.)

   (b) Prove the converse of (a). That is, show that every root of $f$ that belongs to $F$ has the form $\frac{-b+R}{2a}$ for some $R \in F$ satisfying $R^2 = \Delta$.

   *Hint.* Completing the square yields $4af(x) = (2ax + b)^2 - \Delta$.

5. Let $F$ be a field, and let $f(x) \in F[x]$ be a polynomial of degree $n$. Show that $f$ has at most $n$ distinct roots in $F$. *Hint:* Use the Root-Factor theorem.

6. Decide whether each of the following polynomials is irreducible in $F[x]$ for the given field $F$.

   (a) $f(x) = x^2 + \bar{1}$, $F = \mathbb{Z}_5$,

   (c) $f(x) = x^2 + \bar{1}$, $F = \mathbb{Z}_{19}$,

   (e) $f(x) = x^3 + x + \bar{1}$, $F = \mathbb{Z}_2$.

7. (***; MATH 6000 problem**) The field $\mathbb{Q}(x)$ of rational functions with coefficients in $\mathbb{Q}$ is defined by

$$\mathbb{Q}(x) = \left\{ \frac{a(x)}{b(x)} : a(x), b(x) \in \mathbb{Q}[x], b(x) \neq 0 \right\},$$

with operations $\frac{a(x)}{b(x)} + \frac{c(x)}{d(x)} = \frac{a(x)d(x)+b(x)c(x)}{b(x)d(x)}$ and $\frac{a(x)}{b(x)} \cdot \frac{c(x)}{d(x)} = \frac{a(x)c(x)}{b(x)d(x)}$.[1]

   (a) Say that $\frac{a(x)}{b(x)}$ is positive if $a(x) \neq 0$ and the leading coefficients of $a(x)$ and $b(x)$ have the same sign. Check that whether or not $a(x)/b(x)$ is positive is independent of the representation $a(x)/b(x)$.

   (b) Define $\mathbb{Q}(x)^+ = \{\text{positive elements of } \mathbb{Q}(x)\}$. Check that $\mathbb{Q}(x)^+$ has the three properties stated in Axiom O1 from our handout, where $\mathbb{Q}(x)^+$ replaces $\mathbb{Z}^+$ and $\mathbb{Q}(x)$ replaces $\mathbb{Z}$.

   So we have turned $\mathbb{Q}(x)$ into an ordered field and we can define $<$ and $>$ as we are used to doing.

8. (***; MATH 6000 problem**)

   (a) Is $\mathbb{Q}(x)$ Archimedean? That is: If $a(x), b(x) \in \mathbb{Q}(x)^+$, is there always a positive integer $n$ such that

$$\underbrace{a(x) + a(x) + \cdots + a(x)}_{n \text{ times}} > b(x)\,?$$

   Justify your answer.

   (b) Does $\mathbb{Q}(x)$ have the Least Upper Bound Property? That is, does every nonempty subset of $\mathbb{Q}(x)$ that is bounded above have a least upper bound? Justify your answer.

[1] It is to be understood here that $\mathbb{Q}(x)$ is obtained from $\mathbb{Q}[x]$ by applying the equivalence class construction used to obtain $\mathbb{Q}$ from $\mathbb{Z}$. In particular, $a(x)/b(x) = c(x)/d(x)$ precisely when $a(x)d(x) = b(x)c(x)$ in $\mathbb{Q}[x]$.