Math 4000/6000 – Homework #4

posted February 27, 2018; due at the **start of class** on February 28, 2018

> The advance of mathematics has been like the rhythm of an incoming tide: the first wave, with ever slackening speed, reaches its farthest up the sand, hesitates an instant before rushing back to mingle with the following wave, which reaches a little farther than its predecessor, recedes, mingles with its successor, and so on, till the tide turns, and all are swept back to the ocean to await the next tide. In each surge forward there is some remnant of all the tides that went before, though whatever remains may long since have lost its individuality and be no more recognizable for what it was.
> – E.T. Bell

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.

0. Do but do not turn in: Read examples 3 and 4 on pp. 40–41 of the text.

1. Exercise 1.4.10.

2. Exercise 1.4.8.

3. Exercise 1.4.11.

4. (Products and sums of elements of $\mathbb{Z}_m$)

   (a) For the positive integers $m = 1, 2, 3, 4, 5$, find the sum of all of the elements of $\mathbb{Z}_m$. Formulate a general conjecture and then prove that your guess is correct.

   (b) For the primes $p = 2, 3, 5, 7$, find the product of all of the *nonzero* elements of $\mathbb{Z}_p$. Formulate a general conjecture and then prove that your guess is correct.

   Hint: An insightful approach to (a) is to 'try' to pair each element with its additive inverse. The reason 'try' is in scare quotes is because sometimes an element is its own additive inverse, and so your 'pair' is really just one element — can you determine exactly when this happens? A similar strategy will work for (b); here you need to figure out which elements are their own multiplicative inverses.

5. Exercise 1.4.19(a,b).

6. Let R be a ring. A subset $R' \subseteq R$ is called 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 identifications discussed in class, $\mathbb{Z}$ is a subring of $\mathbb{Q}$ and $\mathbb{Q}$ is a subring of $\mathbb{R}$.)

   (a) Let R be a ring. Suppose that R' is a subset of R closed under $+$ and $\cdot$, that R' contains the additive inverse 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 the additive identity of R — call this 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.)

7. (Representing positive rational numbers in "lowest terms") Let $x \in \mathbb{Q}^+$.

   (a) (Existence of a lowest-terms representation) Show that $x = a/b$ for some pair of relatively prime positive integers a and b.

   (b) (Uniqueness) Now suppose that $x = a/b$ and $x = a'/b'$, where a and b are relatively prime positive integers, and a' and b' are also relatively prime positive integers. Show that $a = a'$ and $b = b'$.

8. Prove that $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$. [Since $\sqrt{3} \in \mathbb{R}$, it follows that $\mathbb{Q}[\sqrt{2}]$ is **properly** contained in $\mathbb{R}$, as we claimed in class.]

9. Let R be a ring. If n is a positive integer, we define

$$n_R = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}},$$

   where 1 is the multiplicative identity of R. (Often one writes n instead of n_R if the meaning is clear from context.) For example, if $R = \mathbb{Z}_{11}$, then $103_R = \bar{4}$, while $77_R = \bar{0} = 0$.

   If there is a positive integer n with $n_R = 0$, then the smallest such positive integer is called the *characteristic of* R. If there is no such n, we define the characteristic of R to be 0.

   (a) What is the characteristic of $\mathbb{Z}$? of $\mathbb{Z}_5$? of $\mathbb{Z}_6$? of $\mathbb{R}$? (No justifications necessary.)

   Solution. $\mathbb{Z}$ has characteristic 0, $\mathbb{Z}_5$ has characteristic 5, $\mathbb{Z}_6$ has characteristic 6, and $\mathbb{R}$ has characteristic 0. □

   (b) Prove that if R is a domain, then the characteristic of R is either 0 or a prime number.

   (c) Prove that if R is an ordered domain, then R has characteristic 0.

10. (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 6 above may be helpful.)

    (b) Define a function $N\colon \mathbb{Z}[i] \to \mathbb{R}$ by $N(z) = z \cdot \bar{z}$. 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 if and only if $N(z) = 1$. Then find (with proof) all units in $\mathbb{Z}[i]$.

11. (*) Exercise 1.4.19(c,d)