MATH 4000/6000 – Homework #4

posted February 25, 2022; due March 4, 2022

Answer the questions, then question the answers.
— Glenn Stevens

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. A subset $R' \subset R$ 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 via the maps ϕ discussed in class, $\mathbb{Z}$ is a subring of $\mathbb{Q}$ and $\mathbb{R}$ is a subring of $\mathbb{C}$.)

   (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.)

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

4. Recall from class that $(\cos(\theta) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta)$, for every real number θ and positive integer n.

   By expanding $(\cos(\theta) + i\sin(\theta))^4$, find formulas for $\cos(4\theta)$ and $\sin(4\theta)$ in terms of $\cos(\theta)$ and $\sin(\theta)$.

5. Let $n \in \mathbb{Z}^+$. We say that the complex number z is a *primitive nth root of* 1 if

   (i) $z^n = 1$, and

   (ii) there is no positive integer $m < n$ with $z^m = 1$.

   For example, -1 is a primitive 2nd root of 1, since $(-1)^2 = 1$ but $(-1)^1 \neq 1$.

   Show that a primitive nth root of 1 exists for every n. How many primitive nth roots of 1 are there for $n = 1, 2, 3, 4$?

6. 3.1.2(a), and then
   $f(x) = x^2 + 2x + 2$, $g(x) = x^2 + 1$, $F = \mathbb{Z}_3$

7. (*) Exercise 2.1.16.

8. (*) Let k, n be positive integers. Show that $\cos(2\pi ik/n) + i\sin(2\pi ik/n)$ is a primitive nth root of 1 if and only if $\gcd(k, n) = 1$.