MATH 4000/6000 – Homework #4
posted February 25, 2019; due March 4, 2019

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 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.)

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. (Writing rational numbers in lowest terms) Let a, b be positive integers.

   (a) Show that there are positive integers c, d with $\frac{a}{b} = \frac{c}{d}$ and $\gcd(c, d) = 1$.

   (b) Show that the integers c and d from part (a) are unique.

4. (de Moivre's theorem)

   (a) Our rule from class for multiplying complex numbers implies that if we write z in polar form, say $z = r(\cos\theta + i\sin\theta)$, then

   $$z^n = r^n(\cos(n\theta) + i\sin(n\theta))$$

   for every positive integer n. Show that the same formula holds for integers $n \leq 0$.

   (b) 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. Let $n \in \mathbb{Z}^+$. In this problem, we assume that z is a primitive nth root of 1.

   (a) Show that the elements of the list $1, z, z^2, \ldots, z^{n-1}$ are distinct.

   (b) Prove that every element on the $1, z, z^2, \ldots, z^{n-1}$ is a complex nth root of 1, and that, conversely, every complex nth root of 1 is on this list.

   (c) Show that if $m \in \mathbb{Z}$, then $z^m = 1 \iff n$ divides m.

   (d) Show that if $m \in \mathbb{Z}$, then z^m is a primitive nth root of $1 \iff \gcd(m, n) = 1$.

   (e) How many primitive 10th roots of 1 are there?

7. Given a polynomial $f(z) = z^3 + pz + q$ (with p, q complex numbers), we set

$$\Delta = \frac{q^2}{4} + \frac{p^3}{27}.$$

   As (will be) shown in class, as long as $p \neq 0$, the complex roots of f are the numbers

$$v - \frac{p}{3v}, \quad \text{where } v^3 = A, \quad \text{for } A := -\frac{q}{2} + \sqrt{\Delta}, \qquad \text{(1st set of roots)}$$

   along with the numbers

$$v' - \frac{p}{3v'}, \quad \text{where } v'^3 = B, \quad \text{for } B := -\frac{q}{2} - \sqrt{\Delta}. \qquad \text{(2nd set of roots)}$$

   The goal of this exercise is for you to show that the second set of roots is redundant; every root in the second set is already in the first. (We claimed this in class.)

   (a) Show that $B \neq 0$. Remember we are assuming $p \neq 0$.

   (b) It follows from part (a) that B has three distinct (and nonzero) complex cube roots v'. Show that for each of these roots v', the number $-\frac{p}{3v'}$ is a cube root of A. Then show that if we let $v = -\frac{p}{3v'}$, then $v - \frac{p}{3v} = v' - \frac{p}{3v'}$. [Hence, every root in the second set is already in the first.]

8. Let $\omega = \cos(2\pi/5) + i\sin(2\pi/5)$. Here we describe how to express ω in terms of square roots.

   (a) Show that ω is a root of the polynomial $z^4+z^3+z^2+z+1$. *Hint:* $z^5-1 = (z-1)(z^4+z^3+z^2+z+1)$.

   (b) Show that $\omega + \frac{1}{\omega}$ is a root of the polynomial $u^2 + u - 1$.

   (c) Show that $\omega + \frac{1}{\omega} = \frac{-1+\sqrt{5}}{2}$, where $\sqrt{5}$ means the positive square root of 5.
   Hint: Figure out the sign of $\omega + \frac{1}{\omega}$ by adding the polar forms of ω and $1/\omega$.

   (d) Put $\beta = \frac{-1+\sqrt{5}}{2}$. So in part (c), you showed $\omega + 1/\omega = \beta$. Now show that

$$\omega = \frac{\beta + i\sqrt{4 - \beta^2}}{2},$$

   where $\sqrt{4-\beta^2}$ means the positive square root of $4 - \beta^2$.

   (e) Deduce from (d) that $\cos(2\pi/5) = \frac{\beta}{2}$ and $\sin(2\pi/5) = \frac{1}{2}\sqrt{4-\beta^2}$.

9. Exercise 2.4.6(a,b).

10. (*) Exercise 2.2.16. *Hint:* First, figure out what f does to rational numbers.