Math 4000/6000 – Homework #5

posted October 2, 2015; due at the **start of class** on October 9, 2015

Mathematics is the art of giving the same name to different things. – Henri Poincare

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 $+$ and $\cdot$ as in R, **and** (B) R' contains the multiplicative identity 1_R of 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. Carefully verify that (A) also holds. To get started, show that the additive identity of R — call this 0_R — must belong to R'.

   (b) Let R and S be rings. Suppose $\iota\colon S \to R$ is a one-to-one map that preserves operations and satisfies $\iota(1_S) = 1_R$. Check that the set

   $$\iota(S) := \{\iota(s) : s \in S\}$$

   is a subring of R.

   Example: The map $\iota\colon \mathbb{Z} \to \mathbb{Q}$ given by $n \mapsto \frac{n}{1}$ satisfies the conditions in (b), and hence $\iota(\mathbb{Z})$ is a subring of $\mathbb{Q}$. We usually identify $\mathbb{Z}$ with its image $\iota(\mathbb{Z})$ in $\mathbb{Q}$, which allows us to call $\mathbb{Z}$ a subring of $\mathbb{Q}$. Similar justification can be given for speaking of $\mathbb{Q}$ as a subring of $\mathbb{R}$ or $\mathbb{R}$ as a subring of $\mathbb{C}$.

   (c) 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. (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 $\mathbb{C}$.

   (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 $z, w \in R$.

   (d) Using your work in (b) and (c), find (with proof) all units in $\mathbb{Z}[i]$.

   Hint: First show that $z \in \mathbb{Z}[i]$ is a unit if and only if $N(z) = 1$.

For the next problem, recall that if R is an integral domain, the *fraction field* of R is the field F

$$F = \Big\{\frac{a}{b} : a, b \in R, b \neq 0, \text{where we make the identification } \frac{a}{b} = \frac{c}{d} \text{ if and only if } ad = bc\Big\};$$

addition and multiplication of fractions is defined in the usual way.

3. Let R be an integral domain that is a subring of a field K. Let F be the fraction field of R.

   (a) Show that the map $\iota\colon F \to K$ given by $\frac{a}{b} \mapsto ab^{-1}$ is well defined and is an embedding of F into K.

   (b) Suppose now that R is a field. Let F be the fraction field of R. Show that the map $\iota\colon F \to R$ given by $\frac{a}{b} \to ab^{-1}$ is both an embedding and a bijection.

4. (de Moivre's theorem)

   (a) Let n be an integer. Show that if $z \in \mathbb{C}$ is a nonzero complex number with polar representation $r(\cos\theta + i\sin\theta)$, then for every integer n, the complex number z^n has the polar representation
   $$r^n(\cos(n\theta) + i\sin(n\theta)).$$
   (Don't forget the case of negative integers n!)

   (b) Use part (a) to find formulas for $\cos(4\theta)$ and $\sin(4\theta)$ in terms of $\cos(\theta)$ and $\sin(\theta)$. The binomial theorem may be helpful.

5. (nth roots of complex numbers) Let n be a positive integer. Let w be a nonzero complex number. Show that if $\sqrt[n]{w}$ is any fixed nth root of w, then the set of all nth roots of w consists of the numbers $\zeta \cdot \sqrt[n]{w}$, where ζ runs over the nth roots of 1.

6. 2.3.13.

7. Let p and q be complex numbers with $p \neq 0$. Let $\Delta = \frac{q^2}{4} + \frac{p^3}{27}$. 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 shown in class, as long as $p \neq 0$, the complex roots of f are the numbers
   $$v - \frac{p}{3v}, \quad \text{where } v \text{ runs over the cube roots of} \quad A := -\frac{q}{2} + \sqrt{\Delta}.$$
   Here $\sqrt{\Delta}$ denotes any fixed square root of Δ.

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

   (b) It follows from (a) that A has three distinct (and nonzero) cube roots v. Show that for each of these roots v, the number $-\frac{p}{3v}$ is a cube root of $-\frac{q}{2} - \sqrt{\Delta}$. (This explains why our derivation for the roots of a cubic equation yields three roots and not six!)

8. (A lemma for problem 9) Let p be a nonzero complex number. Show that if v and v' are nonzero complex numbers, then
   $$v - \frac{p}{3v} = v' - \frac{p}{3v'} \iff \text{either } v = v' \text{ or } v = -\frac{p}{3v'}.$$

9. In this exercise and the next you will show that when $f(z) = z^3 + pz + q$,
   $$f \text{ has fewer than 3 distinct roots} \iff \Delta = 0.$$

In this exercise we prove the forward direction. So we assume that f has < 3 distinct roots and we seek to show $\Delta = 0$.

In this problem and the next, we adopt the notation $A := -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ and $A' := -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$.

(a) Prove that $\Delta = 0$ in the case when $p = 0$.

(b) Now assume $p \neq 0$. Using the formula for the roots of f and the result of problem 8, show that if f has fewer than 3 distinct roots, then there are two cube roots v and v' of A for which $v = -\frac{p}{3v'}$.

(c) (continuation) With v, v' as in part (b), use problem 7 to show that v is a cube root of both A and A'. Conclude that $\Delta = 0$.

10. (continuation) Now we treat the reverse implication. Assume $\Delta = 0$.

    (a) Show that if $p = 0$, then $f(z) = z^3$ and f has only one distinct root.

    (b) (continuation) Now assume $p \neq 0$. Show that if v is any cube root of A, then so is $-\frac{p}{3v}$.

    (c) (continuation) Show that one can select a cube root v of A in such a way that $v' := -\frac{p}{3v}$ is distinct from v. Deduce from our formula for the roots of f that f has at most 2 different roots.

11. (*) Exercise 2.2.16.

12. (*) Suppose distinct complex numbers z_1, z_2, z_3 satisfy $z_1^2 + z_2^2 + z_3^2 = z_1 z_2 + z_2 z_3 + z_1 z_3$. Show that z_1, z_2, z_3 are the vertices of an equilateral triangle.