Math 4000/6000 – Homework #6

posted October 10, 2016; due at the **start of class** on October 19, 2016

"Art is fire plus algebra." – Jorge Luis Borges

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. 3.1.2(a), and then
   $f(x) = x^2 + 2x + 2$, $g(x) = x^2 + 1$, $F = \mathbb{Z}_3$
2. 3.1.6.
3. 3.1.10(a,c,e,f).
4. 3.1.15.

   Hint: You may assume, without proof, that the product rule holds for derivatives of polynomials over an arbitrary field. That is, $(fg)' = f'g + fg'$.
5. 3.1.18
6. Let A be an integral domain, and let $a, b \in A$. Show that the following three conditions are all equivalent:
   (a) $a \mid b$ and $b \mid a$,
   (b) $a = b \cdot u$ for some unit u in A,
   (c) $b = a \cdot u'$ for some unit u' in A.

   Remark. Elements a and b that satisfy any one of these equivalent conditions are called **associate elements**.
7. Let A be an integral domain. For $a, b \in A$, we say that $d \in A$ is a **greatest common divisor** (or **gcd**) of a and b if d is a common divisor divisible by every common divisor. (This generalizes the definition we made in class for $A = F[x]$.) Prove that if d is a gcd of a and b, then d' is also a gcd of a and b if and only if $d' = u \cdot d$ for some unit u.
8. Let F be a field.
   (a) Show that the units in $F[x]$ are exactly the nonzero constants.

   Remark. It follows from this problem and Exercise 7 that if $g(x)$ is any one gcd of $a(x)$ and $b(x)$, then all gcds have the form $c \cdot g(x)$, where c is a nonzero constant. Remember that we made this claim in class.

   (b) Let $a(x), b(x) \in F[x]$, not both zero. Show that if $g(x)$ is any gcd of $a(x)$ and $b(x)$, then $g(x) = a(x)X(x) + b(x)Y(x)$ for some $X(x), Y(x) \in F[x]$.

   Hint: You already know this for the particular gcd that is output by the Euclidean algorithm.
9. (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 $\mathbb{C}$. *Hint:* Use Problem 8(a) from your last homework.

(b) Define a function $N\colon \mathbb{C} \to \mathbb{R}$ 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 $z, w \in \mathbb{C}$.

(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 $N(z) = 1$.

10. (More on $\mathbb{Z}[i]$) In this exercise, we outline a proof of the following **division algorithm for** $\mathbb{Z}[i]$:

Division algorithm for $\mathbb{Z}[i]$**:** Let $a, b \in \mathbb{Z}[i]$, with $b \neq 0$. Then there exist $q, r \in \mathbb{Z}[i]$ with
$$a = bq + r, \quad \text{and} \quad N(r) < N(b). \tag{†}$$

Example: Let $a = 10 + i$ and $b = 2 - i$. We have
$$10 + i = (2 - i)\overbrace{(4 + 2i)}^{q} + \overbrace{\ i\ }^{r},$$
where $1 = N(i) < N(2 - i) = 5$.

(a) Explain (perhaps with a picture) why every complex number is within a distance $\frac{\sqrt{2}}{2}$ of some element of $\mathbb{Z}[i]$.
Hint: Think geometrically about the complex plane. Where are the elements of $\mathbb{Z}[i]$ located there?

(b) Given $a, b \in \mathbb{Z}[i]$ with $b \neq 0$, let $Q = a/b$. (Remember that $\mathbb{C}$ is a field, so a/b exists in $\mathbb{Q}$.) From part (a), you can find a Gaussian integer q with $|a/b - q| \leq \frac{\sqrt{2}}{2}$. Prove that if we define $r := a - bq$, then (†) holds. In fact, prove the stronger statement that $N(r) \leq \frac{1}{2}N(b)$.

(c) Find q and r satisfying (†) if $a = 5 + 7i$ and $b = 3 - i$.

11. (*) (An example of elements without a gcd) Let $\sqrt{-3}$ denote the complex number $i\sqrt{3}$. Define $\mathbb{Z}[\sqrt{-3}]$ as $\{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$. Then $\mathbb{Z}[\sqrt{-3}]$ is a subring of $\mathbb{C}$. (This is easy to check, but you are not asked to do so.) Prove that the elements $a = 4$ and $b = 2 + 2\sqrt{-3}$ **do not have a gcd** in $\mathbb{Z}[\sqrt{-3}]$.

Hint: Define a function $N(z)$ on $\mathbb{Z}[\sqrt{-3}]$ by putting $N(z) = z\bar{z}$. You may use without proof that $N(z)$ is nonnegative-integer valued, that $N(z) = 0$ iff $z = 0$, that $N(z) = 1$ iff z is a unit, and that $N(zw) = N(z)N(w)$. (The proofs are the same as for $\mathbb{Z}[i]$.) It may help to first prove the lemma that if $a \mid b$ (in $\mathbb{Z}[\sqrt{-3}]$), then $N(a) \mid N(b)$ (in $\mathbb{Z}$).