Math 4000/6000 – Homework #6

posted October 12, 2015; due at the **start of class** on October 19, 2015

"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. 3.1.8.

4. 3.1.10(a,c,e).

5. 3.1.15.

   Hint: You may assume, without proof, that the product rule holds for derivatives of polynomials over an arbitrary field. That is, $(fg)' = f'g + fg'$.

6. Let A be a commutative ring. Given $a, b \in A$, define the *common divisor* set by

$$CD(a, b) = \{d \in A : d \mid a \text{ and } d \mid b\},$$

   and the *linear combination* set by

$$I(a, b) = \{ax + by : x, y \in A\}.$$

   Show that if $a = bq + r$ (with all of $a, b, q, r \in A$), then

$$CD(a, b) = CD(b, r)$$

   and

$$I(a, b) = I(b, r).$$

7. (continuation) Suppose $a, b \in R$, and suppose there is a finite sequence of equations in R of the form

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} \\ r_{n-2} &= r_{n-1} q_n + r_n, \quad \text{where} \quad r_n = 0. \end{aligned}$$

   Let $d = r_{n-1}$ (the remainder at the next-to-last step). Show that d has all of the following properties:

   (a) $d \mid a$ and $d \mid b$,

(b) if $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

(c) $d = ax + by$ for some $x, y \in A$,

8. Let A be an integral domain. Show that the following 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 differ by a unit factor are called **associate elements**.

9. Recall the following definition: If A is a commutative ring, and $a, b \in A$, 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. (That is, d has properties (a) and (b) from problem 7.)

   (a) Suppose now that A is an integral domain, and let $a, b \in A$. 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.

   (b) Suppose $A = F[x]$, where F is a field. Show that if $a(x)$ and $b(x)$ are elements of $F[x]$, not both 0, then there is a unique gcd of $a(x)$ and $b(x)$ that has leading coefficient 1.

10. (More on $\mathbb{Z}[i]$) Look back at the definition of $\mathbb{Z}[i]$ from your last problem set. Recall that for $z \in \mathbb{Z}[i]$, we defined $N(z) = z\bar{z}$. In this exercise, we outline a proof of the following **division theorem for** $\mathbb{Z}[i]$:

    Division theorem 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 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 $\mathbb{Z}$).

12. (*) Exercise 3.1.24.