Math 4000/6000 – Homework #5

posted October 9, 2018; due at the **start of class** on October 18, 2018

"Mathematics knows no races or geographic boundaries; for mathematics, the cultural world is one country." – David Hilbert

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. Exercise 3.1.13.

2. Exercise 3.1.15. *Hint:* You may assume, without proof, that the product rule holds for derivatives of polynomials over an arbitrary field. That is, $(fg)' = f'g + fg'$.

3. Let F be a field. Recall the definition of the gcd in $F[x]$: a gcd of $a(x), b(x)$ is a common divisor of $a(x)$ and $b(x)$ in $F[x]$ that is divisible by every common divisor.

   Show that if $d(x) \in F[x]$ is a gcd of $a(x), b(x)$, then so is $c \cdot d(x)$ for every nonzero $c \in F$. Conversely, show that every gcd of $a(x), b(x)$ has the form $c \cdot d(x)$ for some nonzero $c \in F$.

4. Let F be a subfield of K, and let $\alpha \in K$. Suppose that α is a root of the irreducible polynomial $p(x) \in F[x]$. Let n be the degree of $p(x)$. Show that every element of $F[\alpha]$ has a *unique* representation in the form

   $$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1},$$

   where $a_0, a_1, \ldots, a_{n-1} \in F$.

   Hint: We [will have] proved this in class without the uniqueness requirement. So your job is (only) to prove uniqueness.

5. Exercise 3.2.2(a,b) *Hint:* First read Examples 2 on p. 97.

6. Exercise 3.2.6(a,c,e)

7. (a) Let F and K be fields, and suppose that the nonconstant polynomial $f(x) \in F[x]$ factors in $K[x]$ as

   $$f(x) = c(x - \alpha_1) \cdots (x - \alpha_d),$$

   where $\alpha_1, \ldots, \alpha_d \in K$. Show that $F[\alpha_1, \ldots, \alpha_d]$ is a field. Then explain why $F[\alpha_1, \ldots, \alpha_d]$ is a splitting field for $f(x)$ over F.

   (b) Let $K = \mathbb{Q}[\sqrt[5]{2}, \cos(2\pi/5) + i\sin(2\pi/5)]$. First, show that K is a field. Then show that K is a splitting field of $x^5 - 2$ over $\mathbb{Q}$.

8. In Chapter 4, we will construct a field K with 4 elements containing $\mathbb{Z}_2$ as subfield. In this exercise, *assume* K is such a field. Then in addition to $0, 1$ from $\mathbb{Z}_2$, the field K has two extra elements; call these α and β.

   (a) Show that $\alpha + 1 = \beta$.

   (b) Show that $\alpha^2 = \beta$.

   (c) Prove that K is a splitting field over $\mathbb{Z}_2$ of the polynomial $x^2 + x + 1 \in \mathbb{Z}_2[x]$.

9. (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 $b = 3 - i$.

10. (*) Exercise 3.1.24.

11. (*) (An example where there is no 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 $\mathbb{Z}[\sqrt{-3}]$, meaning that they have no common divisor in $\mathbb{Z}[\sqrt{-3}]$ divisible by every common divisor.

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 $\mathbb{Z}$).