MATH 4000/6000 – Homework ~~#4~~ #5

posted March 13, 2019; due by 5 PM on March 18, 2019

The essence of mathematics lies in its freedom. – Georg Cantor

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. Let F be a field. Prove that the units in $F[x]$ are precisely the nonzero elements of F.
6. 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 in $F[x]$.

   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 $c \in F$.
7. Let F be a field. Give a detailed proof that every nonconstant polynomial in $F[x]$ can be written as a product of irreducible polynomials. (You are not asked to prove uniqueness in this problem.)
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 $\alpha^2 = \beta$.
9. 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.
10. (*) (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 $\mathbb{Z}$).